



User Manual

SMCD3GN-RRR

DOCSIS 3.0 Wireless Cable Modem Gateway

FASTFIND LINKS

Getting to Know Your Gateway

Installing Your Gateway

Configuring Your Computer for TCP/IP

Configuring Your Gateway

SMC Networks
20 Mason
Irvine, CA. 92618
U.S.A.

Copyright © 2010 SMC Networks
All Rights Reserved

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, or for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of SMC.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Apple and Macintosh are registered trademarks of Apple, Inc. All other brands, product names, trademarks, or service marks are property of their respective owners.

This product (Model :SMCD3GN-RRR) includes software code developed by third parties, including software code subject to the GNU General Public License ("GPL") or GNU Lesser General Public License (LGPL"). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL used in this product, are available to you at <http://gpl.smc.com/>. The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL Code and LGPL Code for this product and the terms of the GPL and LGPL.

SMCD3GN-RRR Wireless Cable Modem Gateway User Manual

Contents

Preface.....	v
Key Features	vi
Document Organization.....	vii
Document Conventions	vii
Safety and Warnings	vii
Typographic Conventions.....	viii
1 Getting to Know Your Gateway	9
Unpacking Package Contents	10
System Requirements	10
Front Panel.....	11
Configuring Wireless Security	13
Rear Panel	13
Restoring Factory Defaults.....	14
2 Installing Your Gateway	15
Finding a Suitable Location	16
Connecting to the LAN	16
Connecting the WAN.....	17
Powering on Your Gateway.....	17
3 Configuring Your Computer for TCP/IP	18
Configuring Microsoft Windows 2000.....	19
Configuring Microsoft Windows XP	20
Configuring Microsoft Windows Vista.....	21
Configuring Microsoft Windows 7	23
Configuring an Apple® Macintosh® Computer	25
4 Configuring Your Gateway	27
Pre-configuration Guidelines	28
Disabling Proxy Settings.....	28
Disabling Proxy Settings in Internet Explorer	28
Disabling Proxy Settings in Firefox.....	28
Disabling Proxy Settings in Safari	29
Disabling Firewall and Security Software	29
Confirming Your Gateway's Link Status	29
Accessing Your Gateway's Web Management	30

Understanding the Web Management Interface Screens	31
Web Management Interface Menus and Submenus	32
System Settings Menu.....	34
Password Settings Menu.....	36
LAN Settings Menu.....	38
Ether Switch Port Control Menu	40
QoS Settings Menu	41
Port Based QoS Menu.....	42
CoS Menu.....	43
DSCP Based QoS Menu	45
Queue Settings Menu	46
DSCP Remarking Menu	48
Wireless Basic Settings Menu	51
Wireless Encryption Settings Menu	53
WPS Setup	56
MAC Filtering.....	59
Adding and Deleting Wireless Client Stations	60
Port Forwarding Menu	61
Adding a Port Forwarding Entry for a Predefined Service	62
Adding a Port Forwarding Entry for a Customer-Defined Service	64
Security Settings (Firewall) Menu.....	67
Enabling or Disabling Firewall	67
Configuring Access Control	69
Configuring Special Applications	74
Configuring URL Blocking	77
Configuring Schedule Rules	79
Configuring Email and Syslog Alerts	80
Configuring DMZ Settings	84
Using the Reboot Menu to Reboot Your Gateway	85
Using the Tools Settings Menu.....	86
Using the Reboot Menu to Reboot the Gateway	87
Viewing Status Information.....	88
Viewing Cable Status Information	90
Appendix A - Specifications	91
Appendix B - Compliances	95
Index	96

Preface

Congratulations on your purchase of your SMCD3GN-RRR Wireless Cable Modem Gateway. Your SMCD3GN-RRR Wireless Cable Modem Gateway is the ideal all-in-one wired and wireless solution for the home or business environment. SMC is proud to provide you with a powerful, yet simple communication device for connecting your local area network (LAN) to the Internet.

This user manual contains all the information you need to install and configure your new SMCD3GN-RRR Wireless Cable Modem Gateway.



Key Features

The following list summarizes your Gateway's key features.

- Integrated, CableLabs-compliant DOCSIS 1.1/ 2.0 /3.0 cable modem
- Four 10/100/1000 Mbps Auto-Sensing LAN ports with Auto-MDI/MDIX
- High-speed 300 Mbps IEEE 802.11n Wireless Access Point
- Dynamic Host Configuration Protocol (DHCP) for dynamic IP configuration, and Domain Name System (DNS) for domain name mapping
- One USB 2.0 port
- IEEE 802.11 b/g/n interoperability with multiple vendors
- Wireless WEP, WPA, and WPA2 encryption, Hide SSID, and MAC Filtering
- VPN pass-through support using PPTP, L2TP, or IPSec
- Advanced SPI firewall Gateway for enhanced network security from attacks over the Internet:
 - Firewall protection with Stateful Packet Inspection
 - Client privileges
 - Hacker prevention
 - Protection from denial of service (DoS) attacks
 - Network Address Translation (NAT)
- Universal Plug and Play (UPnP) enables seamless configuration of attached devices
- Effortless plug-and-play installation
- Intuitive graphical user interface (GUI) configuration, regardless of operating system
- Comprehensive front panel LEDs for network status and troubleshooting
- Compatible with all popular Internet applications

Document Organization

This document consists of four chapters and two appendixes.





- **Chapter 1** - describes the contents in your Gateway package, system requirements, and an overview of your Gateway's front and rear panels.
- **Chapter 2** - describes how to install your Gateway.
- **Chapter 3** - describes how to configure TCP/IP settings on the computer you will use to configure your Gateway.
- **Chapter 4** - describes how to configure your Gateway.
- **Appendix A** - lists your Gateway's specifications.
- **Appendix B** - contains compliance information.

Document Conventions

This document uses the following conventions to draw your attention to certain information.

Safety and Warnings

This document uses the following symbols to draw your attention to certain information.

Symbol	Meaning	Description
	Note	Notes emphasize or supplement important points of the main text.
	Tip	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
	Warning	Warnings indicate that failure to take a specified action could result in damage to the device.
	Electric Shock Hazard	This symbol warns users of electric shock hazard. Failure to take appropriate precautions such as not opening or touching hazardous areas of the equipment could result in injury or death.

Typographic Conventions

This document also uses the following typographic conventions.

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels.
<i>Italic</i>	Indicates a variable, which is a placeholder for actual text provided by the user or system. Angled brackets (< >) are also used to indicate variables.
<code>screen/code</code>	Indicates text that is displayed on screen or entered by the user.
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Italic font is also used to indicate variables.
[] square brackets	Indicates optional values.
{ } braces	Indicates required or expected values.
vertical bar	Indicates that you have a choice between two or more options or arguments.

1 Getting to Know Your Gateway

Before you install your SMCD3GN-RRR Wireless Cable Modem Gateway, check the package contents and become familiar with your Gateway's front and back panels.

The topics covered in this chapter are:

- Unpacking Package Contents (page 10)
- System Requirements (page 10)
- Front Panel (page 11)
- Configuring Wireless Security (page 13)
- Rear Panel (page 13)
- Restoring Factory Defaults (page 14)

Unpacking Package Contents

Your SMCD3GN-RRR package should include the following items:

- One SMCD3GN-RRR Wireless Cable Modem Gateway
- One Power cord
- One Category 5E Ethernet cable
- One CD that contains this User Manual

System Requirements

To complete the installation, you will need the following items:

- Provisioned Internet access on a cable network that supports cable modem service.
- A computer with a wired network adapter with TCP/IP installed.
- A Java-enabled Web browser, such as Microsoft Internet Explorer 5.5 or above.
- Microsoft® Windows® 2000 or higher for USB driver support.

Front Panel

The front panel of your SMCD3GN-RRR Wireless Cable Modem Gateway contains a set of light-emitting diode (LED) indicators. These LEDs show the status of your Gateway and simplify troubleshooting. The front panel also contains a **WPS** button for configuring wireless security automatically.

Figure 1 shows the front panel of your SMCD3GN-RRR Wireless Cable Modem Gateway. Table 1 describes the front panel LEDs.



Figure 1. Front Panel of your SMCD3GN-RRR Wireless Cable Modem Gateway

Table 1. Front Panel LEDs

LED	Color	Description
POWER	Green	ON = power is supplied to your Gateway. OFF = power is not supplied to your Gateway.
DS	Green	Blinking = scanning for DS channel. ON = synchronized on 1 channel only.
	Blue	ON = synchronized with more than 1 channel (DS Bond mode).
DS and US		Both DS and US blinking together = operator is performing maintenance.
US	Green	Blinking = ranging is in progress. ON = ranging is complete on 1 channel only. OFF = scanning for DS channel.
	Blue	ON = ranging is complete, operate with more than 1 channel (US Bond mode).
ONLINE	Green	Blinking = cable interface is acquiring IP, ToD, CM configuration. ON = Gateway is operational. OFF = Gateway is offline.
LINK	Green	Blinking = data is transmitting. ON = Gateway is operational. OFF = no Ethernet link detected.
DIAG	Amber	ON = system failure. OFF = normal operation.
LAN 1 – LAN 4	Green	Blinking = data is transmitting. ON = connected at 10 or 100 Mbps. OFF = no Ethernet link detected.
	Blue	Blinking = data is transmitting. ON = connected at 1 Gbps. OFF = no Ethernet link detected.
WIFI	Green	Blinking = data is transmitting. ON = Wi-Fi is enabled. OFF = Wi-Fi is disabled.
USB	Green	Reserved for future use.

Configuring Wireless Security

The front panel has a **WPS** button for configuring wireless security automatically. Pressing this button for 5 seconds automatically configures wireless security. If the client device supports WPS Push Button Configuration (PBC), press the button within 60 seconds to automatically configure security on the client.

After pressing this button for 5 seconds, the **WPS** LED on the front panel flashes. When a client joins the network successfully, the LED remains ON until the next WPS action or the device reboots. If no client joins, the LED stops blinking after 4 minutes.

Rear Panel

The rear panel of your SMCD3GN-RRR Wireless Cable Modem Gateway contains a reset button and the ports for attaching the supplied power adapter and making additional connections. Figure 2 shows the rear panel components and Table 2 describes their meanings.

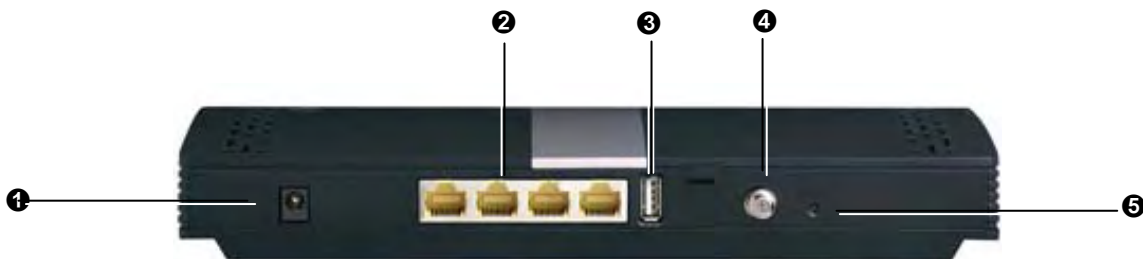


Figure 2. Rear View of your SMCD3GN-RRR Wireless Cable Modem Gateway

Table 2. SMCD3GN-RRR Wireless Cable Modem Gateway Rear Panel Components

	Item	Description
❶	Power (12VDC)	Connect the supplied power cord to this port.
❷	LAN 1-4	Four 10/100/1000 auto-sensing RJ-45 switch ports. Connect devices on your local area network such as a computer, hub, or switch to these ports.
❸	USB	USB 2.0 high-speed port for storing configurations externally.
❹	Cable	Connect your coaxial cable line to this port.
❺	Reset button	Use this button to reset the power or restore the default factory settings (see "Restoring Factory Defaults," below). This button is recessed to prevent accidental resets of your Gateway.

Restoring Factory Defaults

The Reset button on the back panel can be used to return the device to its factory default settings. As a result, any changes made to your Gateway's default settings will be lost.

If you do not have physical access to the device, you can use the GUI to either power cycle the device (See "Using the Reboot Menu to Reboot Your Gateway" on page 85.) or return your Gateway to its factory default settings (see "Using the Reboot Menu to Reboot Your Gateway" on page 85).

The following procedure describes how to use the Reset button to power cycle your Gateway and return it to its original factory default settings.

1. Leave power plugged into your Gateway.
2. Find the Reset button on the back panel, then press and hold it for at least 10 seconds.
3. Release the Reset button.

2 Installing Your Gateway

This chapter describes how to install your SMCD3GN-RRR Wireless Cable Modem Gateway. The topics covered in this chapter are:

- Finding a Suitable Location (page 16)
- Connecting to the LAN (page 16)
- Connecting the WAN (page 17)
- Powering on Your Gateway (page 17)

Finding a Suitable Location

The SMCD3GN-RRR Wireless Cable Modem Gateway can be installed in any location with access to the cable network. All of the cables connect to the rear panel of your Gateway for better organization and utility. The LED indicators on the front panel are easily visible to provide users with information about network activity and status.

For optimum performance, the location you choose should:

- Be close to a working AC power outlet
- Allow sufficient air flow around your Gateway to keep the device as cool as possible
- Not expose your Gateway to a dusty or wet environment
- Be an elevated location such as a high shelf, keeping the number of walls and ceilings between your Gateway and your other devices to a minimum
- Be away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, or the base for a cordless phone
- Be away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal

Connecting to the LAN

Using an Ethernet LAN cable, you can connect your Gateway to a desktop computer, notebook, hub, or switch. Your SMCD3GN-RRR Wireless supports auto-MDI/MDIX, so you can use either a standard straight-through or crossover Ethernet cable.

1. Connect either end of an Ethernet cable to one of the four **LAN** ports on the rear panel of your Gateway (see Figure 3).

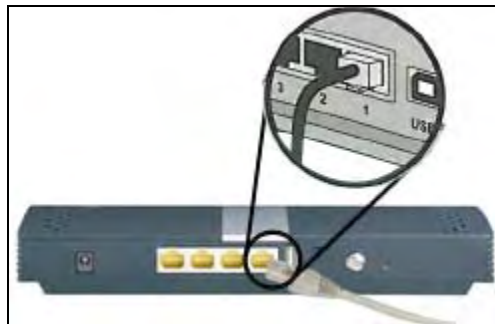


Figure 3. Connecting to a LAN Port on your Gateway Rear Panel

2. Connect the other end of the cable to your computer's network-interface card (NIC) or to another network device (see Figure 4).

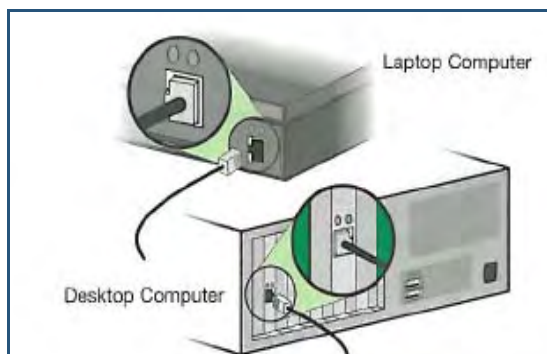


Figure 4. Connecting your Gateway to the a Laptop or Desktop Computer

Connecting the WAN

To connect your Gateway to a Wide Area Network (WAN) interface:

3. Connect a coaxial cable to the port labeled **Cable** on the rear panel of your Gateway from a cable port in your home or office (see Figure 2 on page 13). Use only manufactured coaxial patch cables with F-type connectors at both ends for all connections.
4. Hand-tighten the connectors to secure the connection.

Powering on Your Gateway

After making your LAN and WAN connections, use the following procedure to power on your Gateway:

1. Connect the supplied power cord to the port on the rear panel of your Gateway (see Figure 2 on page 13).
2. Connect the other end of the power cord to a working power outlet. The Gateway powers on automatically, the **POWER** LED on the front panel goes ON, and the other front panel LEDs show your Gateway's status (see Table 1 on page 12).



WARNING: Only use the power cord supplied with your Gateway. Using a different power cord can damage your Gateway and void the warranty.

3 Configuring Your Computer for TCP/IP

After you install your SMCD3GN-RRR Wireless Cable Modem Gateway, configure the TCP/IP settings on a computer that will be used to configure your Gateway. This chapter describes how to configure TCP/IP for various Microsoft Windows and Apple Macintosh operating systems.

The topics covered in this chapter are:

- Configuring Microsoft Windows 2000 (page 19)
- Configuring Microsoft Windows XP (page 20)
- Configuring Microsoft Windows Vista (page 21)
- Configuring Microsoft Windows 7 (page 23)
- Configuring an Apple® Macintosh® Computer (page 25)

Configuring Microsoft Windows 2000

Use the following procedure to configure your computer if your computer has Microsoft Windows 2000 installed.

1. On the Windows taskbar, click **Start**, point to **Settings**, and then click **Control Panel**.
2. In the Control Panel window, double-click the **Network and Dial-up Connections** icon. If the Ethernet adapter in your computer is installed correctly, the **Local Area Connection** icon appears.
3. Double-click the **Local Area Connection** icon for the Ethernet adapter connected to your Gateway. The Local Area Connection Status dialog box appears (see Figure 5).

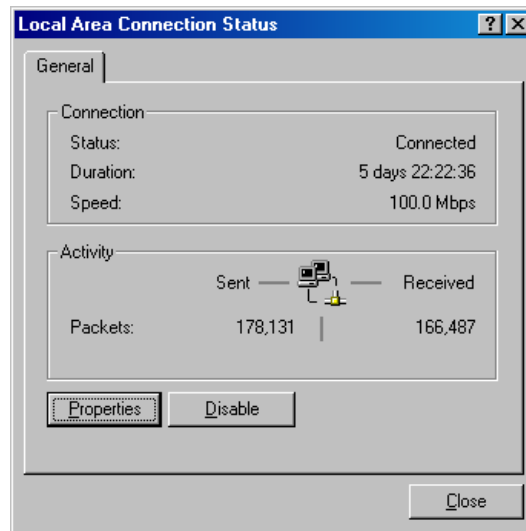


Figure 5. Local Area Connection Status Window

4. In the Local Area Connection Status dialog box, click the **Properties** button. The Local Area Connection Properties dialog box appears.
5. In the Local Area Connection Properties dialog box, verify that **Internet Protocol (TCP/IP)** is checked. Then select **Internet Protocol (TCP/IP)** and click the **Properties** button.
6. Click **Obtain an IP address automatically** to configure your computer for DHCP.
7. Click the **OK** button to save this change and close the Local Area Connection Properties dialog box.
8. Click **OK** button again to save these new changes.
9. Restart your computer.

Configuring Microsoft Windows XP

Use the following procedure to configure a computer running Microsoft Windows XP with the default interface. If you use the Classic interface, where the icons and menus resemble previous Windows versions, perform the procedure under “Configuring Microsoft Windows 2000” on page 19.

1. On the Windows taskbar, click **Start**, click **Control Panel**, and then click **Network and Internet Connections**.
2. Click the **Network Connections** icon.
3. Click **Local Area Connection** for the Ethernet adapter connected to your Gateway. The Local Area Connection Status dialog box appears.
4. In the Local Area Connection Status dialog box, click the **Properties** button (see Figure 6). The Local Area Connection Properties dialog box appears.

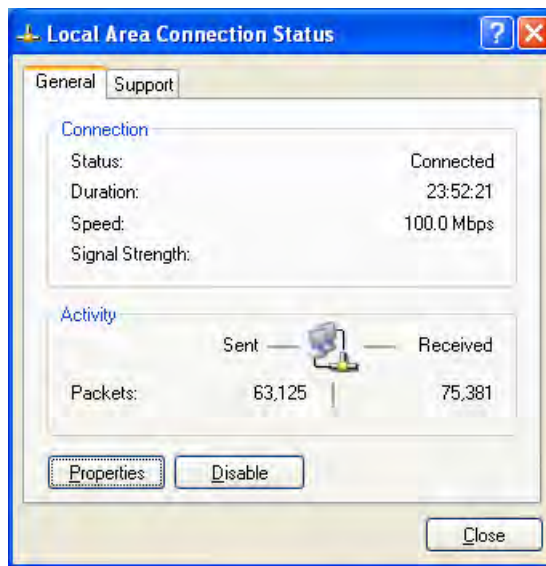


Figure 6. Local Area Connection Status Window

5. In the Local Area Connection Properties dialog box, verify that **Internet Protocol (TCP/IP)** is checked. Then select **Internet Protocol (TCP/IP)** and click the **Properties** button. The Internet Protocol (TCP/IP) Properties dialog box appears.
6. In the Internet Protocol (TCP/IP) Properties dialog box, click **Obtain an IP address automatically** to configure your computer for DHCP. Click the **OK** button to save this change and close the Internet Protocol (TCP/IP) Properties dialog box.
7. Click the **OK** button again to save your changes.
8. Restart your computer.

Configuring Microsoft Windows Vista

Use the following procedure to configure a computer running Microsoft Windows Vista with the default interface. If you use the Classic interface, where the icons and menus resemble previous Windows versions, perform the procedure under “Configuring Microsoft Windows 2000” on page 19.

1. On the Windows taskbar, click **Start**, click **Control Panel**, and then select the **Network and Internet** icon.
2. Click **View Networks Status and tasks** and then click **Management Networks Connections**.
3. Right-click the **Local Area Connection** icon and click **Properties**.
4. Click **Continue**. The Local Area Connection Properties dialog box appears.
5. In the Local Area Connection Properties dialog box, verify that **Internet Protocol (TCP/IPv4)** is checked. Then select **Internet Protocol (TCP/IPv4)** and click the **Properties** button (see Figure 7). The Internet Protocol Version 4 Properties dialog box appears.

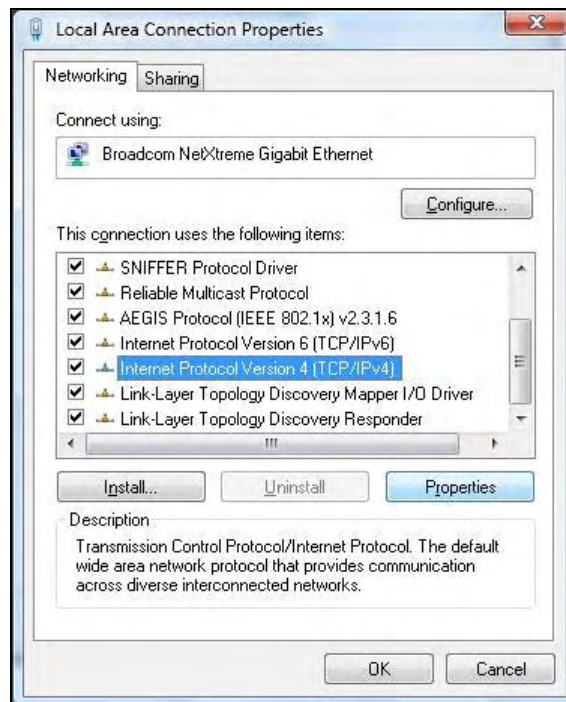


Figure 7. Local Area Connection Properties Window

6. In the Internet Protocol Version 4 Properties dialog box, click **Obtain an IP address automatically** to configure your computer for DHCP (see Figure 8).

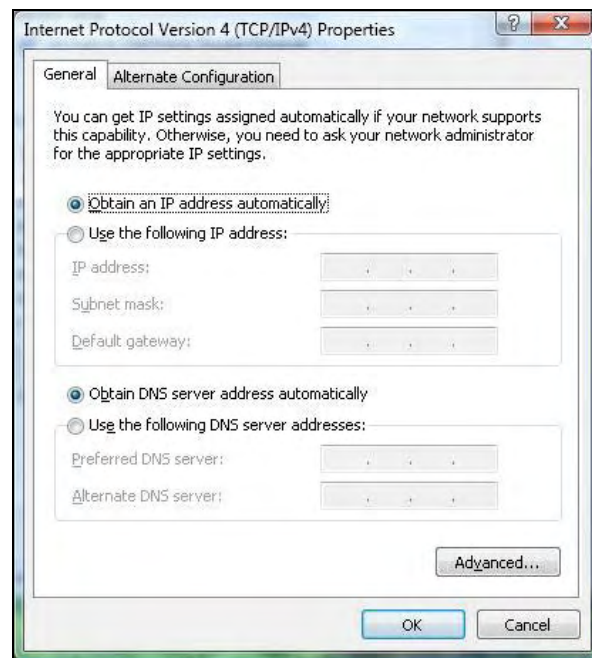


Figure 8. Internet Protocol Properties Window

7. Click the **OK** button to save your changes and close the dialog box.
8. Click the **OK** button again to save your changes.

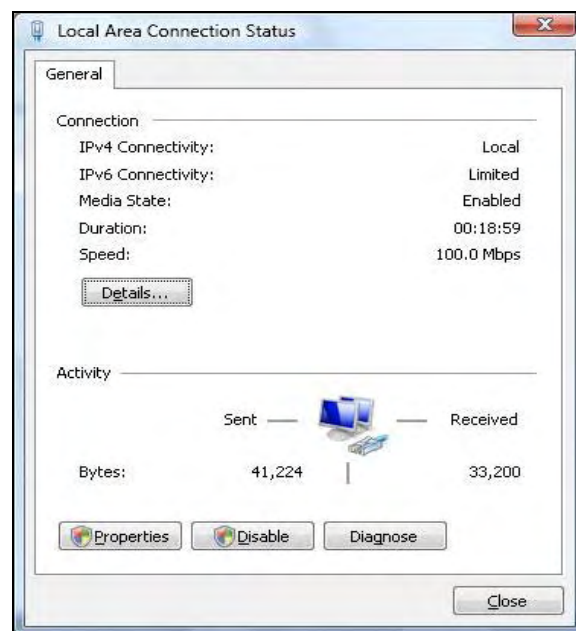


Figure 9. Local Area Connection Status Window

Configuring Microsoft Windows 7

Use the following procedure to configure a computer running Microsoft Windows 7.

1. In the Start menu search box, type: **ncpa.cpl**

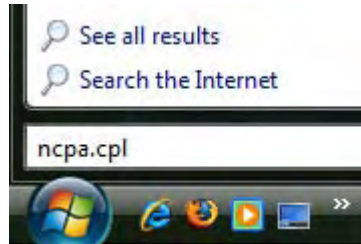


Figure 10. Typing ncpa.cpl in the Start Menu Box

The Network Connections List appears.

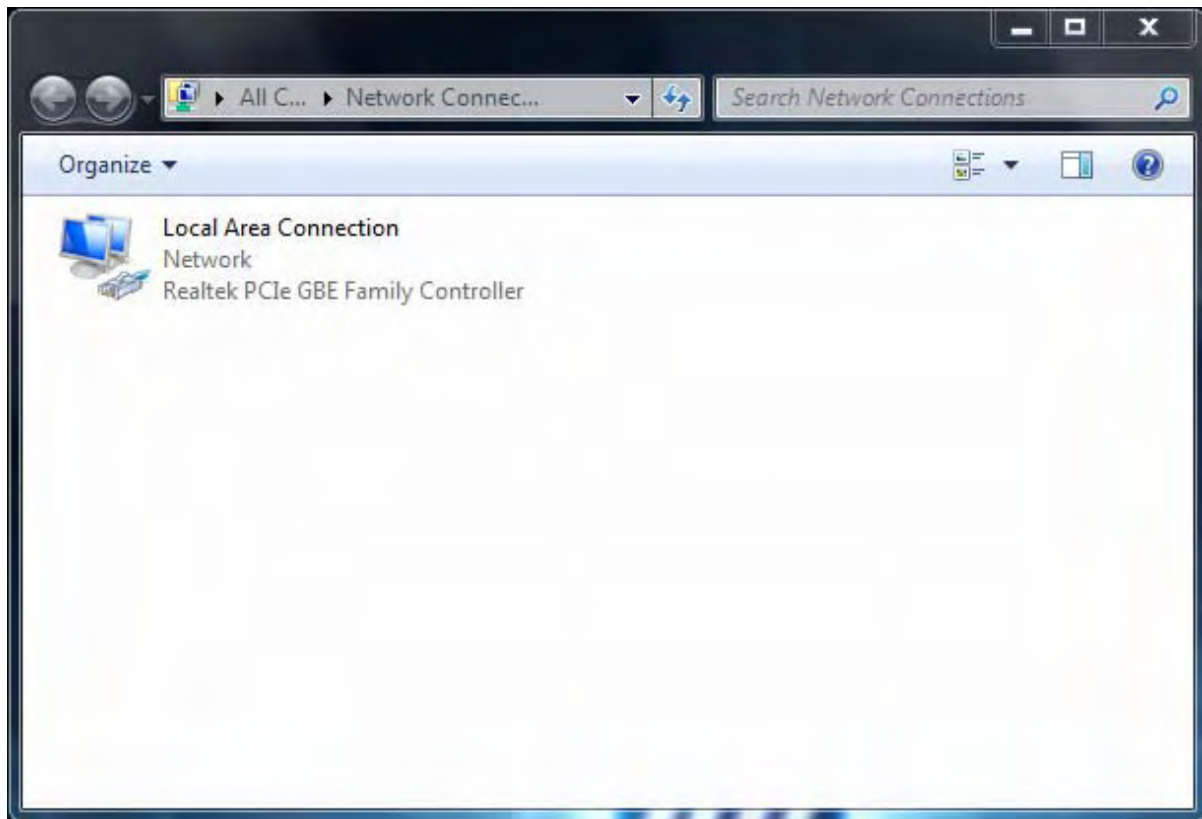


Figure 11. Example of Network Connections List

2. Right-click the **Local Area Connection** icon and click **Properties**.
3. In the **Networking** tab, click either **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.

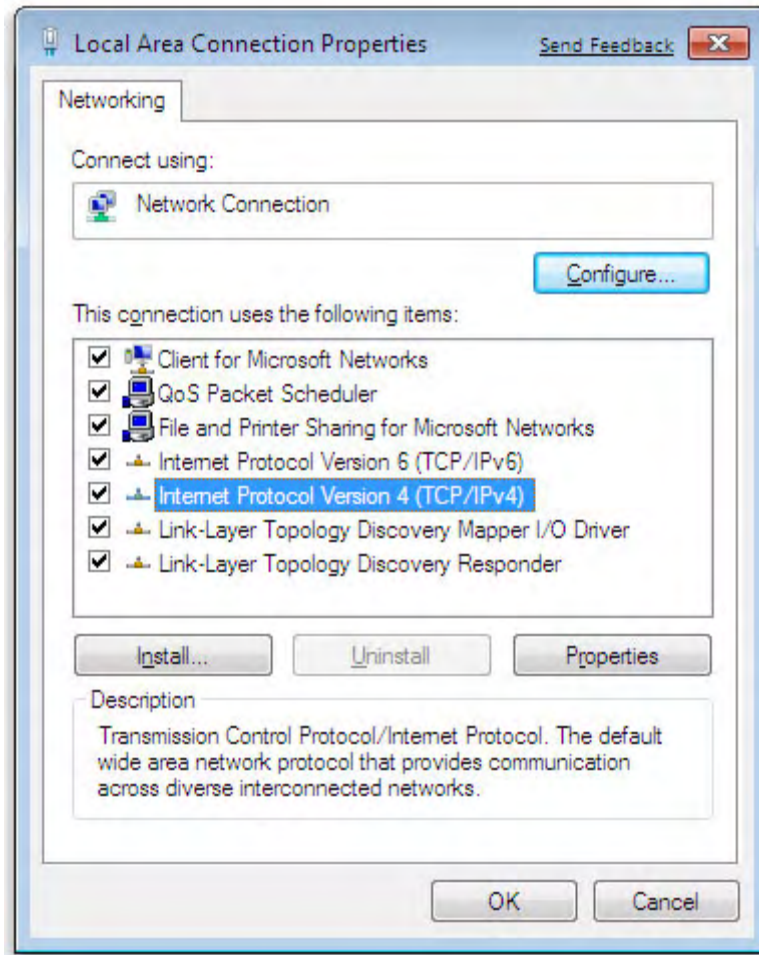


Figure 12. Local Area Network Connection Properties Dialog Box

4. In the properties dialog box, click **Obtain an IP address automatically** to configure your computer for DHCP (see Figure 13).

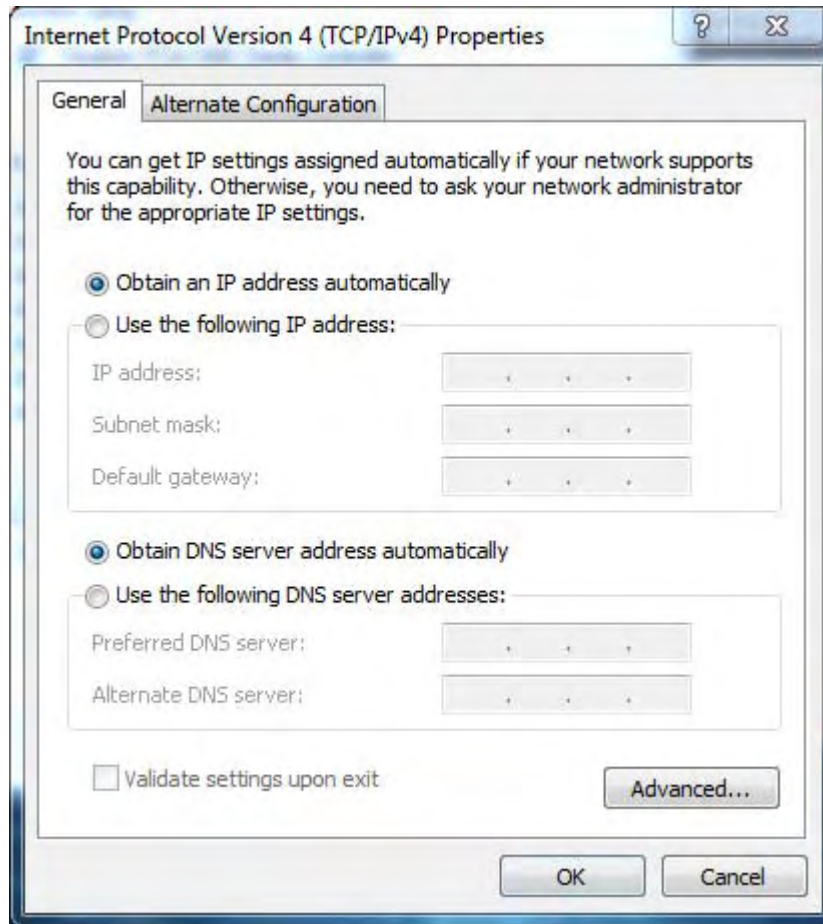


Figure 13. Properties Window

5. Click the **OK** button to save your changes and close the dialog box.
6. Click the **OK** button again to save your changes.

Configuring an Apple® Macintosh® Computer

The following procedure describes how to configure TCP/IP on an Apple Macintosh running Mac OS 10.2. If your Apple Macintosh is running Mac OS 7.x or later, the steps you perform and the screens you see may differ slightly from the following. However, you should still be able to use this procedure as a guide to configuring your Apple Macintosh for TCP/IP.

1. Pull down the Apple Menu, click **System Preferences**, and select **Network**.

2. Verify that the NIC connected to your SMCD3GN-RRR is selected in the **Show** field.
3. In the **Configure** field on the **TCP/IP** tab, select **Using DHCP** (see Figure 14).
4. Click **Apply Now** to apply your settings and close the TCP/IP dialog box.

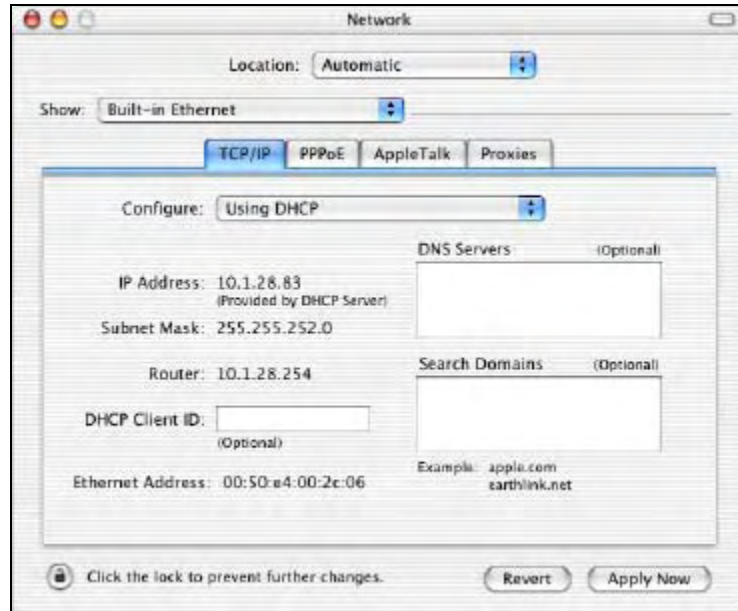


Figure 14. Selecting Using DHCP in the Configure Field

4 Configuring Your Gateway

This chapter describes how to use a Web browser to configure your Gateway.

The topics covered in this chapter are:

- Pre-configuration Guidelines (page 28)
- Accessing Your Gateway's Web Management (page 30)
- Understanding the Web Management Interface Screens (page 31)
- Web Management Interface Menus (page 32)

Pre-configuration Guidelines

Before you configure your Gateway, observe the guidelines in the following sections.

Disabling Proxy Settings

Disable proxy settings in your Web browser. Otherwise, you will not be able to view your Gateway's Web-based configuration pages.

Disabling Proxy Settings in Internet Explorer

The following procedure describes how to disable proxy settings in Internet Explorer 5 and later.

1. Start Internet Explorer.
2. On your browser's **Tool** menu, click **Options**. The Internet Options dialog box appears.
3. In the Internet Options dialog box, click the **Connections** tab.
4. In the **Connections** tab, click the **LAN settings** button. The Local Area Network (LAN) Settings dialog box appears.
5. In the Local Area Network (LAN) Settings dialog box, uncheck all check boxes.
6. Click **OK** until the Internet Options window appears.
7. In the Internet Options window, under **Temporary Internet Files**, click **Settings**.
8. For the option **Check for newer versions of stored pages**, select **Every time I visit the webpage**.
9. Click **OK** until you close all open browser dialog boxes.

Disabling Proxy Settings in Firefox

The following procedure describes how to disable proxy settings in Firefox.

1. Start Firefox.
2. On your browser's **Tools** menu, click **Options**. The Options dialog box appears.
3. Click the **Advanced** tab.
4. In the **Advanced** tab, click the **Network** tab.
5. Click the **Settings** button.
6. Click **Direct connection to the Internet**.
7. Click the **OK** button to confirm this change.

Disabling Proxy Settings in Safari

The following procedure describes how to disable proxy settings in Safari.

1. Start Safari.
2. Click the **Safari** menu and select **Preferences**.
3. Click the **Advanced** tab.
4. In the **Advanced** tab, click the **Change Settings** button.
5. Choose your location from the **Location** list (this is generally **Automatic**).
6. Select your connection method. If using a wired connection, select **Built-in Ethernet**. For wireless, select **Airport**.
7. Click the **Proxies** tab.
8. Be sure each proxy in the list is unchecked.
9. Click **Apply Now** to finish.

Disabling Firewall and Security Software

Disable any firewall or security software that may be running on your computer. For more information, refer to the documentation for your firewall.

Confirming Your Gateway's Link Status

Confirm that the **LINK** LED on your Gateway front panel is ON (see Figure 1 on page 11). If the LED is OFF, replace the Ethernet cable connecting your computer and Gateway.

Accessing Your Gateway's Web Management

After configuring your computer for TCP/IP and performing the preconfiguration guidelines on the previous page, you can now easily configure your Gateway from the convenient Web-based management interface. From your Web browser (Microsoft Internet Explorer version 5.5 or later), you will log in to the interface to define system parameters, change password settings, view status windows to monitor network conditions, and control your Gateway and its ports.

To access your SMCD3GN-RRR Wireless Cable Modem Gateway's web-based management screens, use the following procedure.

1. Launch a Web browser.



Note: The Cable Modem does not have to be online to configure your Gateway.

2. In the browser address bar, type <http://192.168.0.1> and press the Enter key. For example:



The Login User Password screen appears (see Figure 15)



Figure 15. Login User Password Screen

3. In the Login User Password screen, enter the default username and the default password provided by your service provider. Both the username and password are case sensitive.
4. Click the **Login** button to access your Gateway. The Status page appears, showing connection status information about your Gateway.

Understanding the Web Management Interface Screens

The left side of the management interface contains a menu bar you use to select menus for configuring your Gateway. When you click a menu, information and any configuration settings associated with the menu appear in the main area of the interface (see Figure 16). If the displayed information exceeds what can be shown in the main area, scroll bars appear to the right of the main area so you can scroll up and down through the information.

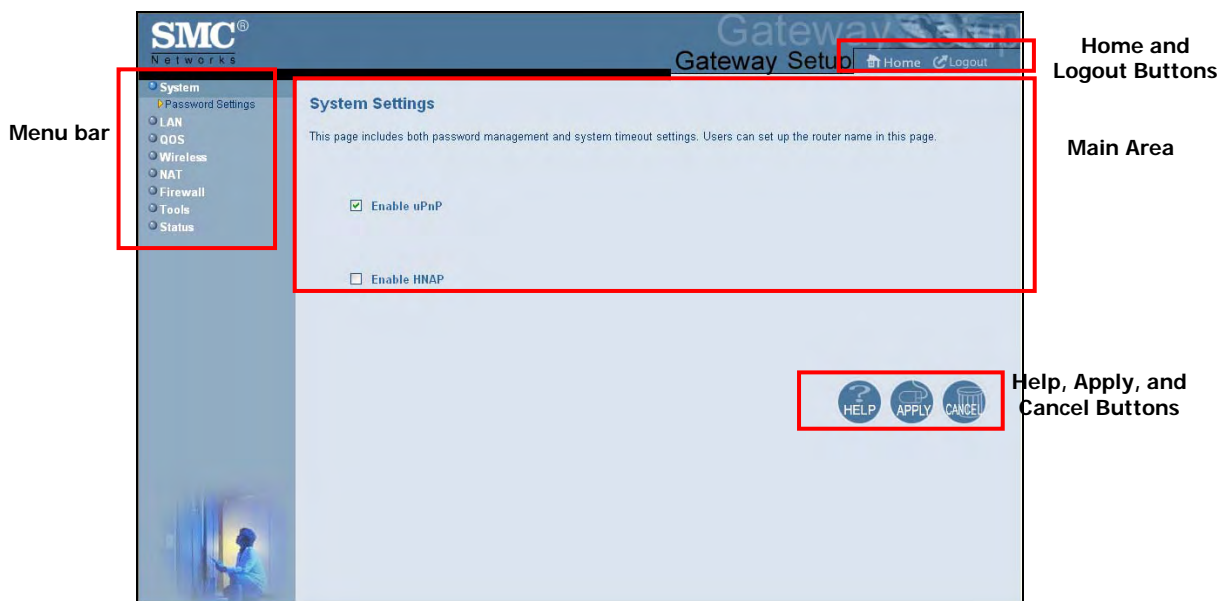


Figure 16. Main Areas on the Web Management Interface

Some menus have submenus associated with them. If you click a menu that has submenus, the submenus appear below the menu. For example, if you click the **System** menu, the submenu **Password Settings** appears below the **System** menu (see Figure 17).

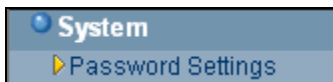


Figure 17. Example of System Submenu

The top-right side of the page contains a **Home** button that displays the Home (Status) page and a **Logout** button for logging out of the Web management interface.

The bottom right side of the screen contains three buttons:

- **Help** displays online help
- **Apply** saves your configuration changes to the displayed page
- **Cancel** discards any configuration changes made to the current page

Web Management Interface Menus and Submenus

Table 3 describes the menus and submenus in the Web management interface.

Table 3. Web Management Interface Menus and Submenus

Menus and Submenus	Description	See Page
System	Lets you enable or disable Universal Plug and Play (uPnP and Home Network Administration Protocol (HNAP). The submenu lets you:	34
System > Password Settings	<ul style="list-style-type: none"> Define the password for logging in to the Gateway's Web interface. 	36
LAN	Lets you configure private LAN IP settings for the Gateway. The submenu lets you:	38
LAN > Ether Switch Control	<ul style="list-style-type: none"> Specify fixed speed and duplex settings, and disable individual LAN ports. 	40
QoS	Lets you configure Quality of Service (QoS) settings. If you enable QoS, the following submenus become available for:	41
QoS > Port	<ul style="list-style-type: none"> Prioritizing performance of the four Gateway LAN ports. 	42
QoS > COS	<ul style="list-style-type: none"> Defining four queues to which the Class of Service (CoS) is mapped. 	43
QoS > DSCP	<ul style="list-style-type: none"> Defining the QoS class queue to which the customized DSCP is mapped. 	45
QoS > Queue	<ul style="list-style-type: none"> Specifying whether QoS behavior runs with strict or weighted priority. 	46
QoS > DSCP Remarking	<ul style="list-style-type: none"> Defining the DSCP remarking action and mode. 	48
Wireless	Lets you enable or disable your Gateway for wireless operation. If wireless is enabled, you can select the wireless mode that your Gateway will use and use the following submenus to:	51
Wireless > Encryption	<ul style="list-style-type: none"> Use encryption to protect the data transmitted across your wireless network. 	53
Wireless > WPS	<ul style="list-style-type: none"> Enable or disable Wi-Fi Protected Setup (WPS). 	56
Wireless > MAC Filtering	<ul style="list-style-type: none"> Allow all wireless client stations or only trusted PCs to connect over a wireless connection. 	59

Table 3. Web Management Interface Menus and Submenus

Menus and Submenus	Description	See Page
NAT > Port Forwarding	Configure predefined and custom port forwarding settings to let Internet users access local services such as the Web Server or FTP server at your local site.	61
Firewall	Lets you enable or disable your Gateway's firewall. Submenus let you:	67
Firewall > Access Control	<ul style="list-style-type: none"> Block traffic at your Gateway's LAN interfaces from accessing the Internet. 	69
Firewall > Special Application	<ul style="list-style-type: none"> Detect port triggers for detect multiple-session applications and allow them to pass the firewall. 	74
Firewall > URL Blocking	<ul style="list-style-type: none"> Block access to certain Web sites from local computers by entering either a full URL address or keywords of the Web site. 	77
Firewall > Schedule Rule	<ul style="list-style-type: none"> Define schedule rules that work with your Gateway's URL blocking feature. 	79
Firewall > Email/Syslog Alert	<ul style="list-style-type: none"> Send email notifications or add entries to the syslog when traffic is blocked, attempts are made to intrude onto the network, and local computers try to access block URLs. 	80
Firewall > DMZ	<ul style="list-style-type: none"> Configure a local client computer for unrestricted two-way Internet access by defining it as a Virtual DMZ host. 	84
Tools > Reboot	Reboot your Gateway.	85
Status	Shows the connection status of your Gateway interfaces, firmware, hardware version numbers, illegal attempts to access your network, and information about DHCP client PCs current connected to your Gateway. The submenu lets you:	88
Status > Cable Status	<ul style="list-style-type: none"> View cable initialization procedures, and cable downstream and upstream status. 	90

System Settings Menu

The System Settings menu lets you enable or disable UPnP and HNAP.

To access the System Settings menu, click **System** in the menu bar. Figure 18 shows an example of the menu and Table 4 describes the setting you can select.

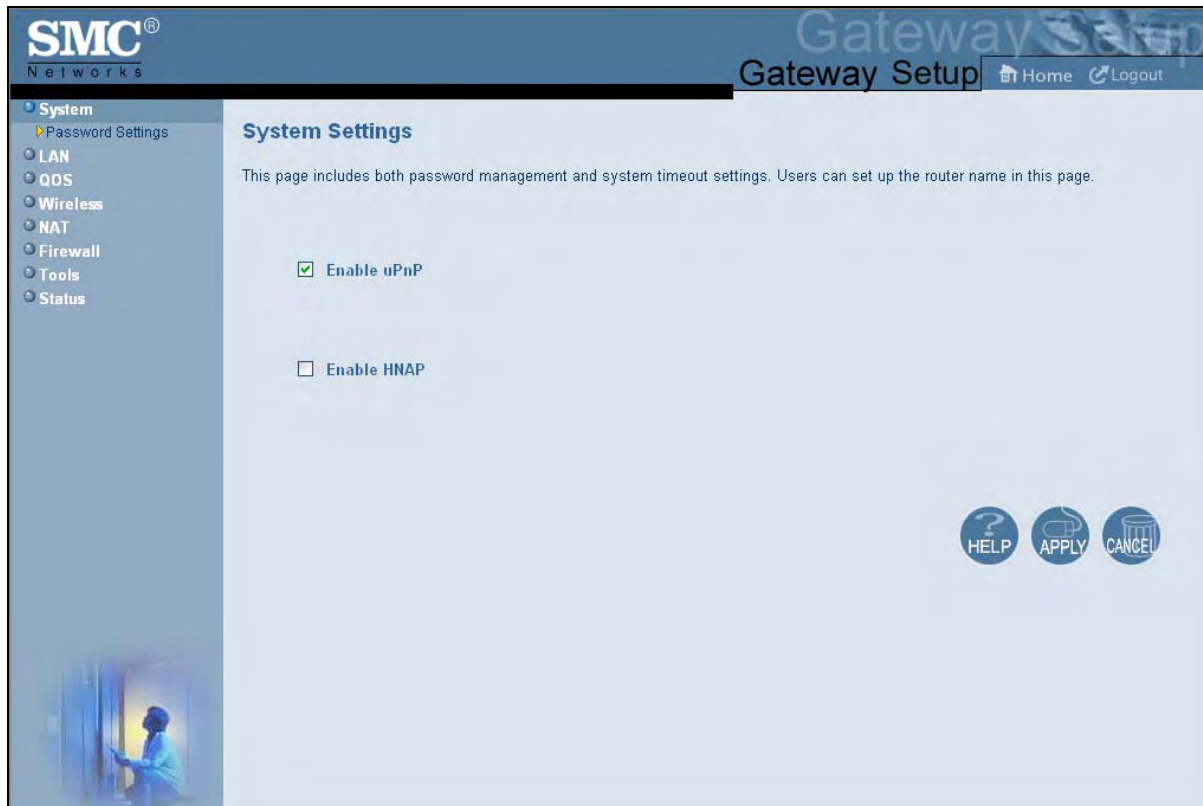


Figure 18. System Settings Menu

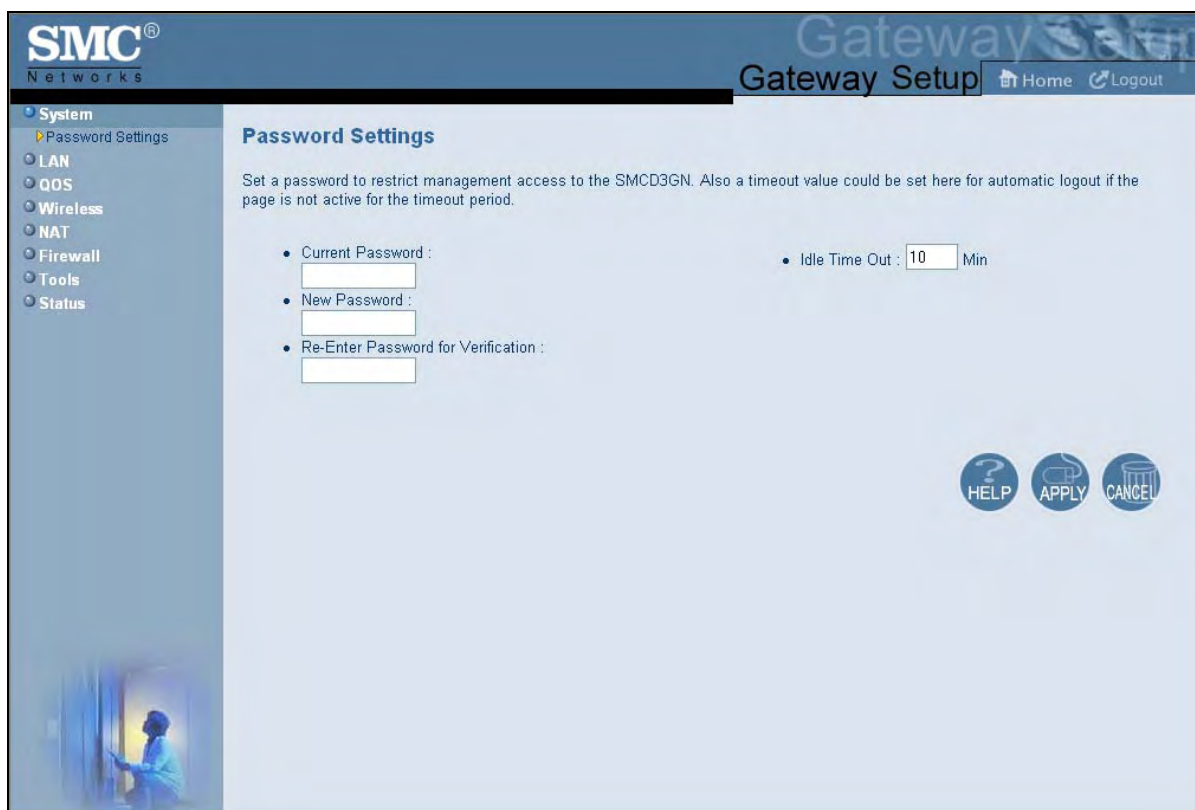
Table 4. System Settings Menu Option

Option	Description
Enable UPnP	<p>Configures your Gateway as a uPnP Internet gateway. UPnP allows for dynamic connectivity between devices on a network. A UPnP-enabled device like your Gateway can obtain an IP address, advertise its capabilities, learn about other connected UPnP devices and then communicate directly with those devices. The same device can end its connection cleanly when it wishes to leave the UPnP community. The intent of UPnP is to support zero-configuration, "invisible" networking of devices including intelligent appliances, PCs, printers, and other smart devices using standard protocols.</p> <ul style="list-style-type: none"> • Checked = uPnP is enabled on your Gateway. (<i>default</i>) • Unchecked = uPnP is disabled on your Gateway.
Enable HNAP	<p>Configures the Gateway as a HNAP device. HNAP allows the Gateway to be configured and managed by remote entities, such as Network Magic or any software application that discovers and manages network devices.</p> <ul style="list-style-type: none"> • Checked = HNAP is enabled on the Gateway. • Unchecked = HNAP is disabled on the Gateway. (<i>default</i>)

Password Settings Menu

The Password Settings menu lets you change the default username and password used to log in to the Gateway's Web interface. The Password Settings menu also lets you change the number of minutes of inactivity that can occur before your Web management session times out automatically. The default setting is 10 minutes.

To access the Password Settings menu, click **System** in the menu bar and then click the **Password Settings** submenu. Figure 19 shows an example of the menu and Table 5 describes the settings you can select.



The screenshot displays the SMC Networks Gateway Setup interface. The top header includes the SMC Networks logo and the title "Gateway Setup". A navigation bar contains "Home" and "Logout" links. A left sidebar lists menu items: System, Password Settings (selected), LAN, QoS, Wireless, NAT, Firewall, Tools, and Status. The main content area is titled "Password Settings" and contains the following text: "Set a password to restrict management access to the SMCD3GN. Also a timeout value could be set here for automatic logout if the page is not active for the timeout period." Below this text are three input fields: "Current Password:", "New Password:", and "Re-Enter Password for Verification:". To the right of these fields is an "Idle Time Out:" setting with a value of "10" and the unit "Min". At the bottom right of the main area are three circular buttons labeled "HELP", "APPLY", and "CANCEL". A small image of a person in a white lab coat is visible in the bottom left corner of the interface.

Figure 19. Password Settings Menu

Table 5. Password Settings Menu Options

Option	Description
Current Password	Enter the current case-sensitive login password. For security purposes, every typed character appears as a dot (•). The default password is not shown for security purposes.
New Password	Enter the new case-sensitive login password you want to use. A password can contain up to 32 alphanumeric characters. Spaces count as password characters. For security purposes, every typed character appears as a dot (•).
Re-Enter Password for Verification	Enter the same case-sensitive login password you typed in the New Password field. For security purposes, every typed character appears as a dot (•).
Idle Time Out	Your Web management interface sessions timeout after 10 minutes of idle time. To change this duration, enter a new timeout value.

LAN Settings Menu

IP addresses are close to being used up and thus very hard to get. One solution to this problem is "private" IP addresses. Private IP addresses are ranges of IP addresses set aside expressly for use by a company or other entity internally. Private IP addresses are non-routable and, therefore, cannot be used to connect directly to the Internet.

Some of the advantages of private IP addresses include:

- Increased security, since private IP addresses are not routable across the Internet
- You conserve the world-wide pool of IP addresses
- You do not have to register or pay for these IP addresses in any way

The LAN Settings menu lets you configure private LAN IP settings for your Gateway. To access the LAN Settings menu, click **LAN** in the menu bar. Figure 20 shows an example of the menu and Table 6 describes the settings you can select.

SMC Networks Gateway Setup Home Logout

LAN Settings

Users can set up the private LAN IP in this page. The private LAN IP is also the IP of the DHCP server which will dynamically allocate IP address for the client PCs behind the Gateway.

Private LAN IP

IP address	192	168	0	1
IP Subnet Mask	255	255	255	0
Domain Name	phub.net.cable.rogers.c			
Enable DHCP Server	<input checked="" type="checkbox"/>			
Lease Time	One Week			

HELP APPLY CANCEL

Figure 20. LAN Settings Menu

Table 6. LAN Settings Menu Options

Option	Description
IP Address	IP address of your Gateway's private LAN settings. Default IP address is 192.168.0.1. If you change this setting, your Gateway reboots after displaying a message.
IP Subnet Mask	Subnet mask of your Gateway's private LAN settings. Default subnet mask is 255.255.255.0.
Domain Name	Domain name of your Gateway's private LAN settings.
Enable DHCP Server	Enables or disables the DHCP server to allow automatic allocation of IP addresses to LAN client PCs. <ul style="list-style-type: none"> • Checked = DHCP server is enabled. (<i>default</i>) • Unchecked = DHCP server is disabled.
Lease Time	Amount of time a DHCP network user is allowed connection to your Gateway with their current dynamic IP address. Default is One Week. This option is available when Enable DHCP Server is checked.

Ether Switch Port Control Menu

By default, the Gateway LAN ports are enabled to auto-negotiate the highest supported speed and appropriate duplex mode. If these settings prevent the Gateway from successfully connecting with other devices, you can use the Ether Switch Port Control menu to configure the Gateway to use fixed speed and duplex settings. The Ether Switch Port Control menu also let you disable the individual LAN ports. For your convenience, each port can be configured independently of the other LAN ports on the Gateway.

To access the Ether Switch Control menu, click **LAN** in the menu bar and then click the **Ether Switch Control** submenu in the menu bar.



Figure 21. Ether Switch Port Control Menu

The following procedure describes how to change the settings in the Ether Switch Port Control menu.

1. To change a port from auto-negotiation to a fixed speed and duplex setting:
 - a. Uncheck the **Auto** check box for the port.
 - b. Under **Speed (10/100/1000)**, click the radio that corresponds to the fixed speed you want to use for that port.
 - c. Under the **Mode H/F** column, leave the check mark for full-duplex mode or uncheck it for half-duplex mode.
2. To disable a port, regardless of the auto-negotiation and duplex settings, uncheck **Enable** for the port.
3. Click **Apply**.

QoS Settings Menu

Quality of Service (QoS) refers to a collection of techniques for identifying data whose delivery across the network is time sensitive, and managing its delivery through both bandwidth allocation and prioritization schemes.

Using the QoS Settings menu, you can enable the Gateway's QoS module to provide guarantees on the ability of the network to deliver predictable results. To access the QoS menu, click **QOS** in the menu bar. Figure 22 shows an example of the menu.

By default, QoS is disabled. To enable the Gateway's QoS module, check **Enable QOS Module** and click **Apply**. To disable the Gateway's QoS module, uncheck **Enable QOS Module** and click **Apply**.

If you enable the Gateway's QoS module, the following submenus appear under **QOS** in the menu bar:

- **Port** - lets you configure the priority queue to which the switch port is mapped. See page 42.
- **COS** - lets you define four queues to which the CoS is mapped. See page 43.
- **DSCP** - lets you define the QoS class queue to which the customized DSCP is mapped. See page 45.
- **Queue** - lets you specify whether QoS behavior runs with strict or weighted priority. See page 46.
- **DSCP Remarking** - lets you define the DSCP remarking action and mode. See page 48.

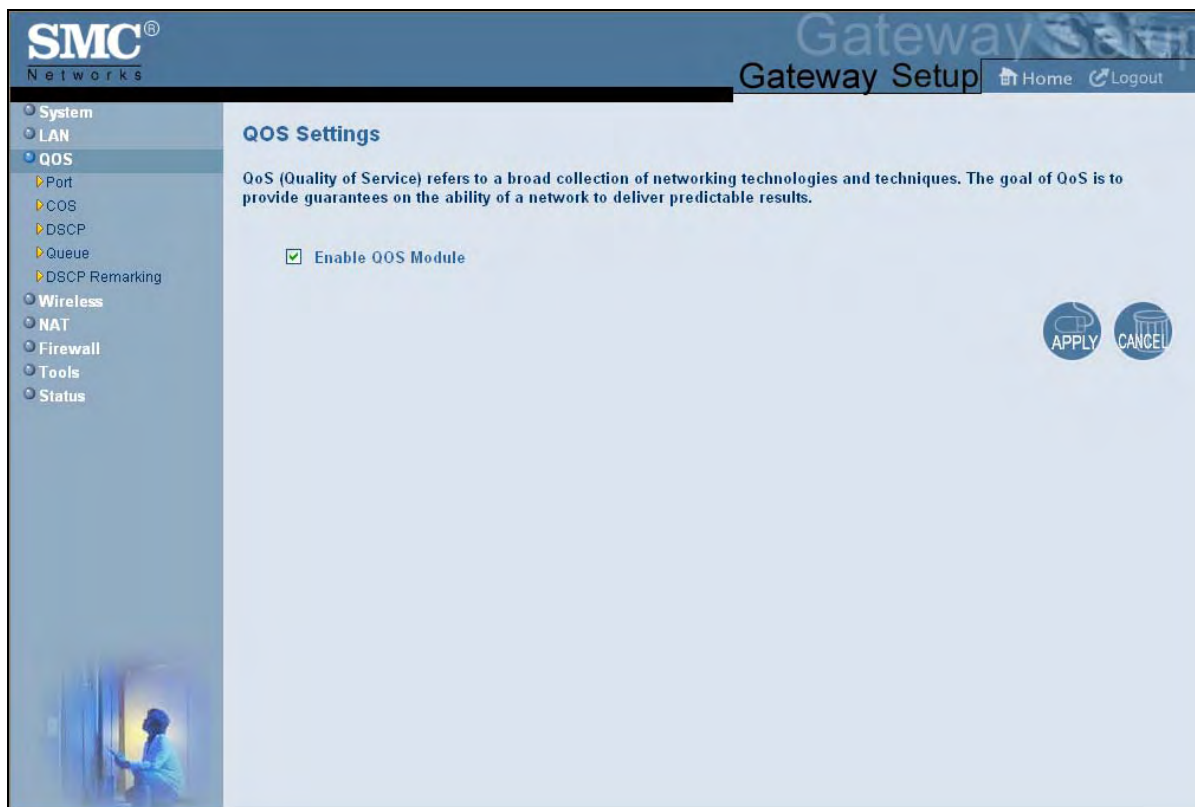


Figure 22. QoS Settings Menu

Port Based QoS Menu

The Port Based QoS menu lets you prioritize performance of the four Gateway LAN ports. To access the Port Based QoS menu, click **QoS** in the menu bar and then click the **Port** submenu in the menu bar. Figure 23 shows an example of the menu.



Note: The **Port** submenu is not available in the menu bar if **Enable QoS Module** is not checked in the QoS Settings menu (see page 41).

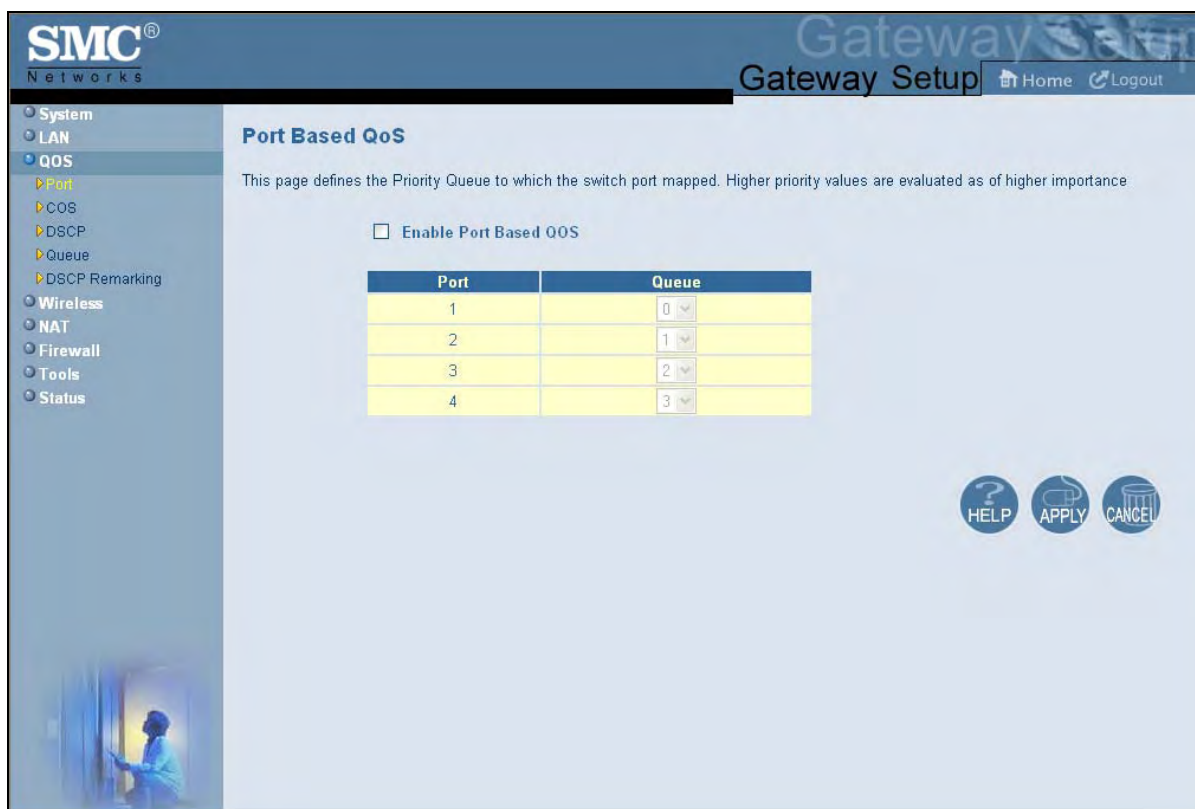


Figure 23. Port Based QoS Menu

To define port-based QoS settings:

1. Check **Enable Port Based QoS**.
2. For each port, select a priority queue number from 0 to 3. Higher priority values are evaluated as being of higher importance than lower priority values.
3. Click **Apply**.

CoS Menu

Given that there will always be points in the network where multiple traffic streams merge or where network links will change speed and capacity, it is important to move traffic on the basis of relative importance. Without CoS prioritization, less important traffic can consume network bandwidth and slow down or halt the delivery of more important traffic. For example, without CoS, most traffic received by the Gateway is forwarded with the same priority it had upon entering the Gateway. In many cases, such traffic is “normal” priority and competes for bandwidth with all other normal-priority traffic, regardless of its relative importance to your requirements. CoS helps to keep the most important network traffic moving at an acceptable speed, regardless of current bandwidth usage. This means you can manage available bandwidth so that the switch transmits the most important traffic first.

The CoS menu lets you configure a CoS priority of 0 through 7 for an outbound packet. When the packet is then sent to a port, the CoS priority determines which outbound queue the packet uses. After configuring CoS priority for outbound packets, use this menu to map the classes of service to the Gateway's four ports.

To access the CoS menu, click **QOS** in the menu bar and then click the **CoS** submenu in the menu bar. Figure 24 shows an example of the menu.



Note: The **COS** submenu is not available in the menu bar if **Enable QoS Module** is not checked in the QoS Settings menu (see page 41).

CoS Settings (802.1p)

This page defines the four queues to which the CoS priority is mapped.

☐ Enable QoS Class based on CoS

Class of Service	Queue
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0

Port Default CoS:

Port	Class of Service
1	1
2	3
3	5
4	7

HELP APPLY CANCEL

Figure 24. CoS Menu

To define CoS settings:

1. Check **Enable QoS Class based on CoS**.
2. For each class of service, assign a queue number from 0 to 3. Higher priority values are evaluated as being of higher importance than lower priority values.
3. Under **Port Default CoS**, map the Gateway's four ports to the classes of service you defined in the previous step.
 - CoS setting from 0 to 3 = normal priority. Packets in this queue leave the port after the high-priority queue is emptied.
 - CoS setting from 4 to 7 = high priority. Packets in this queue leave the port first.
4. Click **Apply**.

DSCP Based QoS Menu

The DSCP Based QoS menu lets you classify and prioritize traffic using DSCP tags. DSCP allows the Gateway to determine how traffic classes should be prioritized. Using the DSCP Based QoS menu, you can use DSCP to provide different levels of service to conforming and non-conforming traffic by appropriately selecting the DSCP values in this menu. The Gateway uses the Hierarchical Token Bucket queuing algorithm, which divides the 64 possible DSCP code values into 8 queues.

Table 7 shows the actual queuing.

Table 7. Queuing for DSCP-Based QoS

Name	Precedence	DSCP Range	Priority
Routing (default)	000 (0)	000000(0) – 000111 (7)	8
Priority	001 (1)	001000 (8) – 001111 (15)	7
Immediate	010 (2)	010000 (16) – 010111 (23)	6
Flash	011 (3)	011000 (24) – 011111 (31)	5
Flash Override	100 (4)	100000 (32) – 100111 (39)	4
Critical	101 (5)	101000 (40) – 101111 (47)	3
Internetwork Control	110 (6)	111000 (48) – 110111 (55)	2
Network Control	111 (7)	111000 (56) – 111111 (63)	1

To access the DSCP Based QoS menu, click **QOS** in the menu bar and then click the **DSCP** submenu in the menu bar. Figure 25 shows an example of the menu.



Note: The **DSCP** submenu is not available in the menu bar if **Enable QOS Module** is not checked in the QoS Settings menu (see page 41).



Figure 25. DSCP Based QoS Menu

To define DSCP-based QoS settings:

1. Check Enable DSCP Based QoS.
2. For each index, select a DSCP value from 0 to 63.
3. Under **Queue**, select a queue (from 0 to 3) you want to map to this DSCP value. Higher priority values are evaluated as being of higher importance than lower priority values.
4. To define DSCP-based QoS values for other queues, repeat steps 2 and 3.
5. Click **Apply**.

Queue Settings Menu

The Queue Settings menu lets you configure QoS behavior as either strict priority or weighted priority.

- Strict priority – allows delay-sensitive data such as voice to be sent before packets in other queues.
- Weighted priority – lets you assign each queue with a certain weight indicating the amount of guaranteed capacity, with high priority packets served before any low priority packets.

To access the Queue Settings menu, click **QOS** in the menu bar and then click the **Queue** submenu in the menu bar. Figure 26 shows an example of the menu.



Note: The **Queue** submenu is not available in the menu bar if **Enable QoS Module** is not checked in the QoS Settings menu (see page 41).

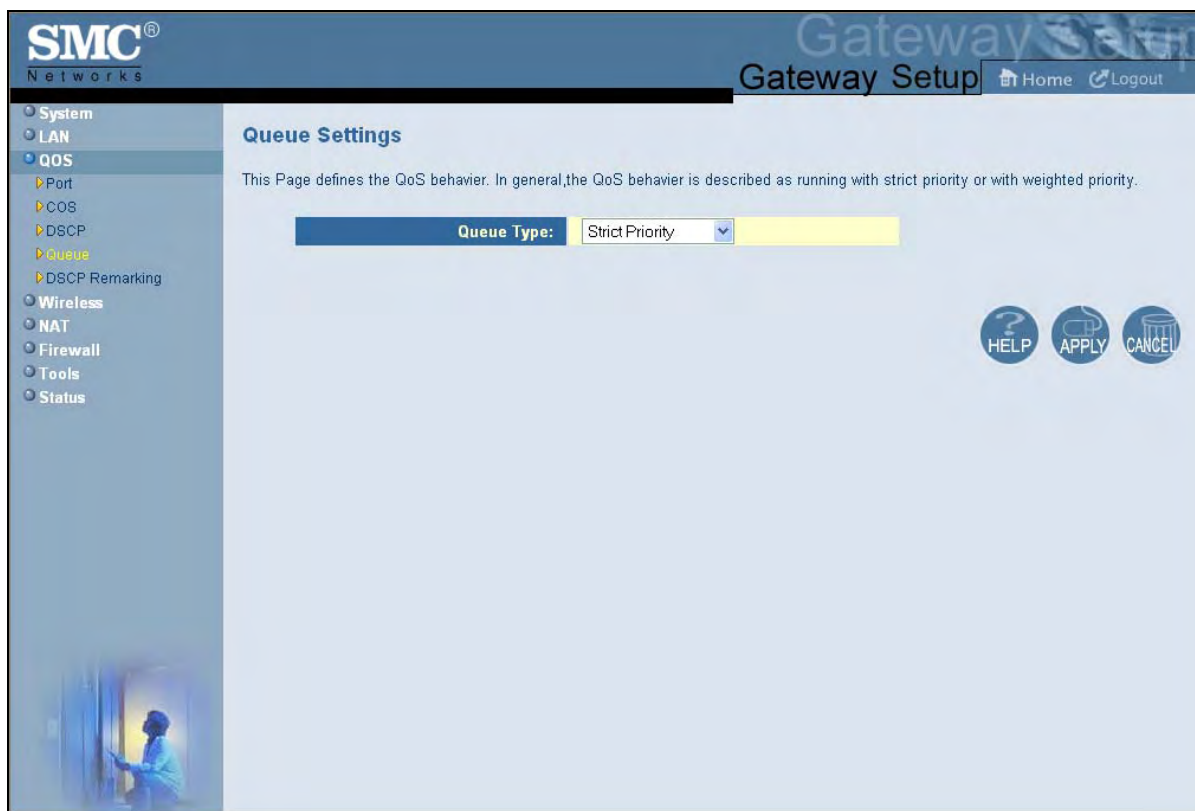


Figure 26. Queue Settings Menu

By default, the Gateway uses strict priority. To change to weighted priority:

1. For **Queue Type**, select **Weighted Priority**. The options in Figure 27 appear.

Queue Type: Weighted Priority		
Weight Base: 10		
Queue	Weight (0-undefined)	% of Bandwidth
0	<input type="text" value="1"/>	10
1	<input type="text" value="2"/>	20
2	<input type="text" value="3"/>	30
3	<input type="text" value="4"/>	40

Figure 27. Weighted Priority Options

2. For **Weight Base**, select a queue weight to ensure that some sets of queues get higher thresholds than others. Queue weight directs the Gateway to set the queue thresholds proportionately. Choices are **8** or **10**. Queues with a weight of 10 are longer than those with a queue weight of 8.
3. For each Gateway queue, select a weight. Each weight corresponds to a percentage of consumed bandwidth, as shown in the **% of Bandwidth** column.
4. When you finish, click **Apply**.

DSCP Remarking Menu

The DSCP Remarking menu lets you configure the Gateway's DSCP remarking mode and actions.

To access the Queue Settings menu, click **QOS** in the menu bar and then click the **DSCP Remarking** submenu in the menu bar. Figure 28 shows an example of the menu.



Note: The **DSCP Remarking** submenu is not available in the menu bar if **Enable QOS Module** is not checked in the QoS Settings menu (see page 41).

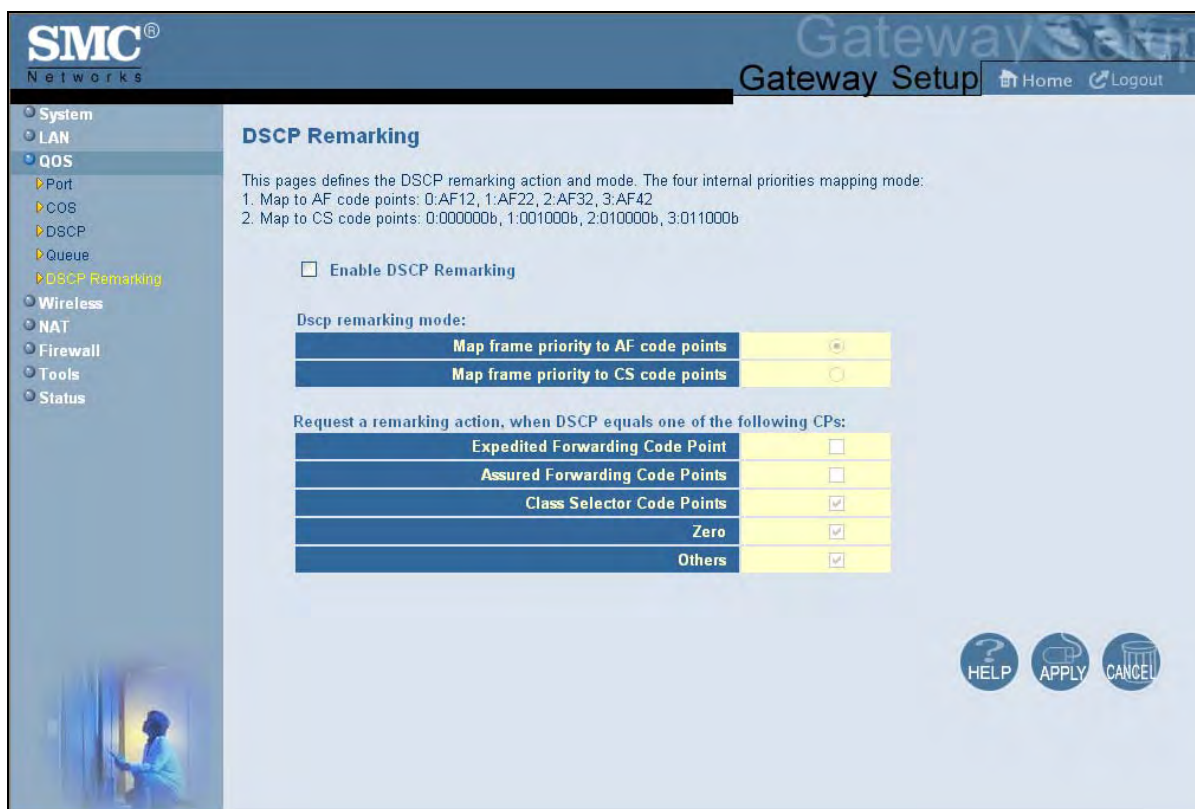


Figure 28. DSCP Remarking Menu

To configure DSCP remarking settings:

1. Check Enable DSCP Remarking.
2. Complete the options in the menu and refer to Table 8.
3. When you finish, click **Apply**.

Table 8. DSCP Remarking Options

Option	Description
Dscp remarking mode	<p>Lets you select the DSCP remarking mode that the Gateway is to use. Choices are:</p> <ul style="list-style-type: none"> • Map frame priority to AF code points = select this option for Quality of Service configurations that use assured forwarding (AF) code points to mark packets. AF guarantees a certain amount of bandwidth to an AF class and allows access to extra bandwidth, if available. (<i>default</i>) • Map frame priority to CS code points = select this option for Quality of Service configurations that use class selector (CS) code points to mark packets. CS provides code points that can be used for backward compatibility with IP Precedence. IP Precedence is a legacy technology that the Gateway supports for backwards compatibility.
Request a remarking action when DSCP equals one of the following CPs	
Expedited Forwarding Code Point	<p>Expedited forwarding provides a low-loss, low-latency, low-jitter, and assured bandwidth service. Applications such as VoIP, video, and other time sensitive applications require a robust network treatment like expedited forwarding. When checked, the Gateway requests a remarking action if DSCP equals an expedited forwarding code point. By default, this option is not checked.</p>

Option	Description
Assured Forwarding Code Points	Assured forwarding defines a method by which packets can be given different forwarding assurances. Traffic can be divided into different classes and then each class given a certain percentage of bandwidth. For example, one class could have 50% of the available link bandwidth, another class could have 30%, and another 20% of the bandwidth. When checked, the Gateway requests a remarking action if DSCP equals an assured forwarding code point. By default, this option is not checked.
Class Selector Code Points	Class Selector code points are code points that can be used for backward compatibility with IP Precedence models. When checked, lets the Gateway request a remarking action if DSCP equals a class selector code point. By default, this option is checked, but does not take effect until the OSPF Status changes to ENABLE.
Zero	When checked, lets the Gateway request a remarking action if DSCP equals zero. By default, this option is checked, but does not take effect until the OSPF Status changes to ENABLE.
Others	When checked, lets the Gateway request a remarking action if DSCP equals a non-zero value. By default, this option is checked, but does not take effect until the OSPF Status changes to ENABLE.

Wireless Basic Settings Menu

The Wireless Basic Settings menu lets you configure basic wireless settings, such as:

- Enabling or disabling the Gateway's wireless operation
- Selecting a wireless mode
- Configuring primary and multiple SSIDs
- Configuring channel settings

To access the Wireless Basic Settings menu, click **Wireless** in the menu bar. Figure 29 shows an example of the menu and Table 9 describes the settings you can select.

SMC® Networks Gateway Setup Home Logout

Wireless Basic Settings

The gateway can be quickly configured as a wireless access point for roaming clients by setting the access identifier and channel number. It also supports data encryption and client filtering. Users could also choose which mode would be run for this access point. There are 11n, 11g, 11n, or mixed mode. If necessary, users can also disable the wireless module by choosing from the **Wireless ON/OFF** drop-down menu.

Wireless ON/OFF	ENABLE			
Wireless Mode	11B/G/N Mixed			
SSID setting	SSID name	hidden	in-service	WMM Mode
Primary SSID	D3GN_SSID0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Channel	11			

HELP APPLY CANCEL

Figure 29. Wireless Basic Settings Menu

Table 9. Wireless Basic Settings Menu Options

Option	Description
Wireless ON/OFF	<p>Enables or disables the Gateway's wireless operation.</p> <ul style="list-style-type: none"> • ENABLE = Gateway's wireless operation is active. Selecting this option activates the options in this menu. Clicking Apply displays the submenus below the Wireless menu. • DISABLE = Gateway's wireless operation is not active. Selecting this option deactivates the options in this menu. Clicking Apply hides the submenus below the Wireless menu. (<i>default</i>)
Wireless Mode	<p>If wireless operation is enabled for the Gateway, this option selects the wireless mode used by the Gateway. Choices are:</p> <ul style="list-style-type: none"> • 11B/G Mixed = use this setting if you have a combination of IEEE 802.11b and IEEE 802.11g devices on your network. • 11B Only = use this setting if you have only IEEE 802.11b devices on your network or want to limit your network to IEEE 802.11b devices. • 11G Only = use this setting if you have only IEEE 802.11g devices on your network or want to limit your network to IEEE 802.11g devices. • 11N Only = use this setting if you have only IEEE 802.11n devices on your network or want to limit your network to IEEE 802.11n devices. • 11G/N Mixed = use this setting if you have a combination of IEEE 802.11g and IEEE 802.11n devices on your network. • 11B/G/N Mixed = use this setting if you have a combination of IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n devices on your network. (<i>default</i>)
SSID setting	<p>SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alpha-numeric characters, which may be any keyboard character. Be sure these settings are the same for all devices in your wireless network. The primary SSID can be hidden, in-service, and configured for Wi-Fi Multimedia (WMM) mode.</p> <ul style="list-style-type: none"> • Hidden = when checked, hides the SSID. Use this setting to block illegal connections. Users cannot reconnect automatically or manually to a wireless network that uses a hidden SSID. The wireless network that uses a hidden SSID does not appear in the Microsoft Windows Wireless Network Connection window. • In-service = when checked, broadcasts the Gateway's SSID. • WMM Mode = when checked, enables WMM. Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.
Channel	<p>Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11 (in North America). Default is Auto, which selects the appropriate channel automatically. All devices in your wireless network must use the same channel to work properly.</p>

Wireless Encryption Settings Menu

Using the Wireless Encryption Settings menu, you can protect the data transmitted across your wireless network. The same encryption keys you specify here must also be configured on your other wireless client devices on your wireless network. To access the Wireless Encryption Settings menu, click **Wireless** in the menu bar and then click the **Encryption** submenu.

Figure 30 shows an example of the menu and Table 10 describes the settings you can select.



Note: The **Encryption** submenu is not available in the menu bar if wireless operation is disabled in the Wireless Basic Settings menu (see page 40).

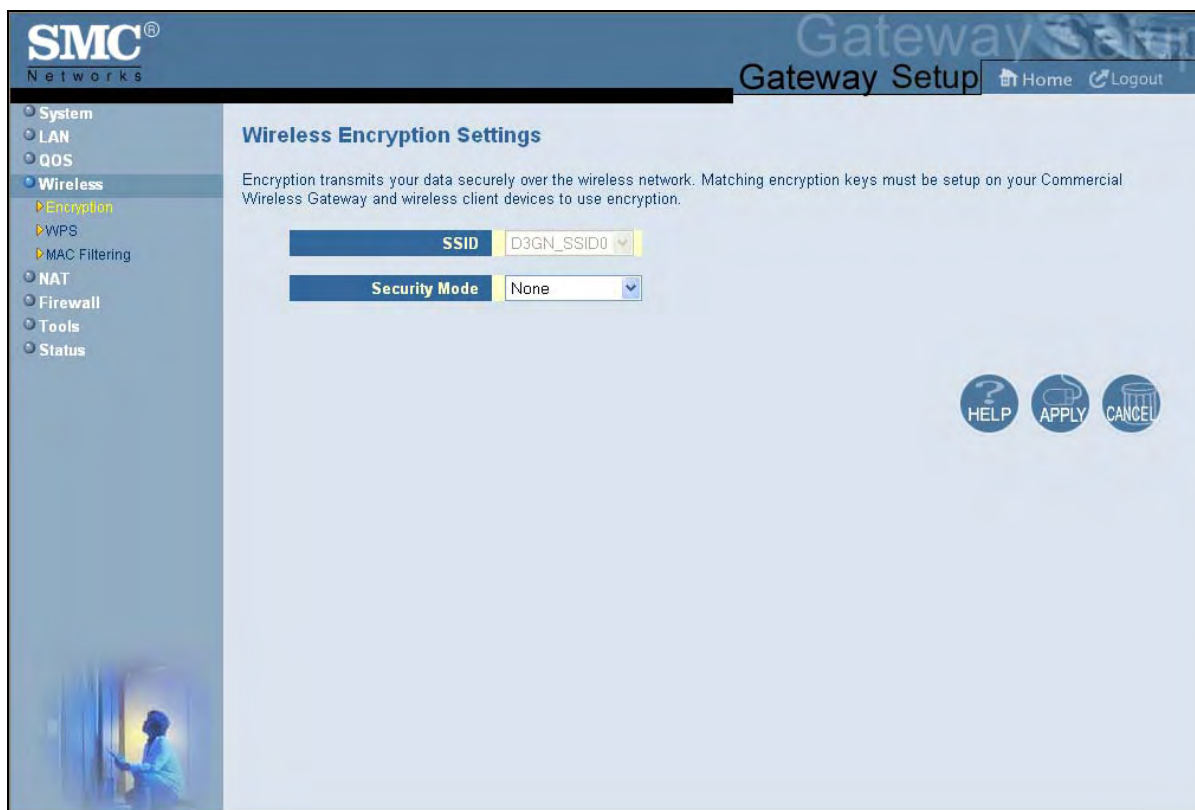


Figure 30. Wireless Encryption Settings Menu

Table 10. Wireless Encryption Settings Menu Options

Option	Description
SSID	Network name of the of the primary wireless carrier. This field can be changed by administrators, but not by users.
Security Mode	<p>Selects the security mode used to protect transmissions across the wireless network.</p> <ul style="list-style-type: none"> • None = no security is used over the wireless network. • WEP = Wired Equivalency Privacy encryption is used over the wireless network. Select this option if your wireless adapters support WEP but not WPA-Personal. WEP provides basic security, but is not as secure as WPA-Personal. If you select WEP, select the options in Figure 31 and Table 11. • WPA-Personal = select this option if your wireless adapters support WPA-Personal. This encryption method is superior to WEP and offers two cipher types, TKIP and AES, with dynamic encryption keys. If you select WPA-Personal, select the options in Figure 32 and Table 12. (default)

Wireless Encryption Settings

Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Commercial Wireless Gateway and wireless client devices to use encryption.

SSID

D3GN_SSID0

Security Mode

WEP

WEP

WEP Key Length	64 bit (10 hex digits)	(length applies to all keys)
WEP Key 1	<input type="text" value="0000000000"/>	
WEP Key 2	<input type="text" value="0000000000"/>	
WEP Key 3	<input type="text" value="0000000000"/>	
WEP Key 4	<input type="text" value="0000000000"/>	
Default WEP Key	WEP Key 1	
Authentication	Open System	
Passphrase	<input type="text"/>	<input type="button" value="Generate Keys"/>

Figure 31. WEP Options

Table 11. WEP Options

Option	Description
WEP Key Length	Level of WEP encryption applied to all WEP keys. Choices are 64-bit (10 hex digits) and 128-bit (26 hex digits).
WEP Key 1 – WEP Key 4	Fields for entering up to four WEP keys manually. Alternatively, you can click the Generate Keys button to generate these keys automatically.
Default WEP Key	Specifies which of the four WEP keys the Gateway is to use as its default.
Authentication	Authentication used. Choices are: <ul style="list-style-type: none"> • Open System = clients can only associate to the wireless access point using Open Option. • Shared Key = all wireless stations share the same secret key. • Automatic = clients can associate to the wireless access point using Open System or Shared Key.
Passphrase	A sequence of words or text that can be used to automatically generate WEP keys. A passphrase can consist of from 8 to 63 ASCII characters. You can use upper-case, lower-case, and numeric characters to form your passphrase. A Generate Keys button next to this field lets the Gateway generate a passphrase based on the characters typed in this field.

Wireless Encryption Settings

Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Commercial Wireless Gateway and wireless client devices to use encryption.

SSID	D3GN_SSID0
Security Mode	WPA-Personal
WPA_Personal	
WPA Mode	WPA-PSK
Cipher type	TKIP
Group Key Update Interval	3600 (seconds)
Pre-shared Key	00000000
Pre-Authentication	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Figure 32. WPA_Personal Options

Table 12. WPA_Personal Options

Option	Description
WPA Mode	Lets administrators select the WPA mode they want to use. Choices are: <ul style="list-style-type: none"> WPA-PSK = select this setting if your access points and wireless clients support WPA-Pre-Shared Key (PSK) Authentication. WPA2-PSK = select this setting if your access points and wireless clients support WPA2-PSK Authentication. Auto (WPA-PSK or WPA2-PSK) = select this setting if your access points and wireless clients support either WPA-PSK or WPA2-PSK. <i>(default)</i>
Cipher type	Algorithm encryption to be used. Choices are: <ul style="list-style-type: none"> TKIP = automatic encryption with WPA-PSK; requires pre-shared key. AES = automatic encryption with WPA2-PSK; requires pre-shared key. TKIP and AES = uses both TKIP and AES cipher types; requires pre-shared key. <i>(default)</i>
Group Key Update Interval	Number of seconds that instructs the Gateway how often it should change the encryption keys. Usually the security level is higher if you set the period shorter to change encryption keys more often. Default value is 3600 seconds (6 minutes). Type 0 to disable group key update interval.
Pre-shared Key	Shared secret between the Gateway and access points and wireless clients. Please check whether your service provider uses a default pre-shared key.
Pre-Authentication	Enables secure fast roaming, without noticeable signal latency. By default, this option is disabled.

WPS Setup

Using the WPS Setup menu, you can enable or disable WPS. WPS is a standard for easy and secure wireless network set up and connections.

The advantages of WPS are:

- WPS automatically configures the network name (SSID) and WPA security key for the Gateway and for the access point and wireless devices that join the network.
- You do not need to know the network name and security keys or passphrases to use WPS to join a wireless network.
- No one can guess your security keys or passphrase because they are generated randomly.
- WPS uses the Extensible Authentication Protocol (EAP), which is a strong authentication protocol used in WPA2.

The disadvantages of WPS are:

- Unless all the Wi-Fi devices on the network are WPS-compatible, you cannot take advantage of the ease of securing the network.
- Not all wireless equipment supports WPS.

- If your wireless devices do not support WPS, it can be hard to join a network that was set up with WPS because the wireless network name and security key are random sequences of letters and numbers.

To access the WPS Setup menu, click **Wireless** in the menu bar and then click the **WPS** submenu. Figure 33 shows an example of the menu. Using the **WPS Config** drop-down list, select the appropriate option to enable or disable WPS setup.

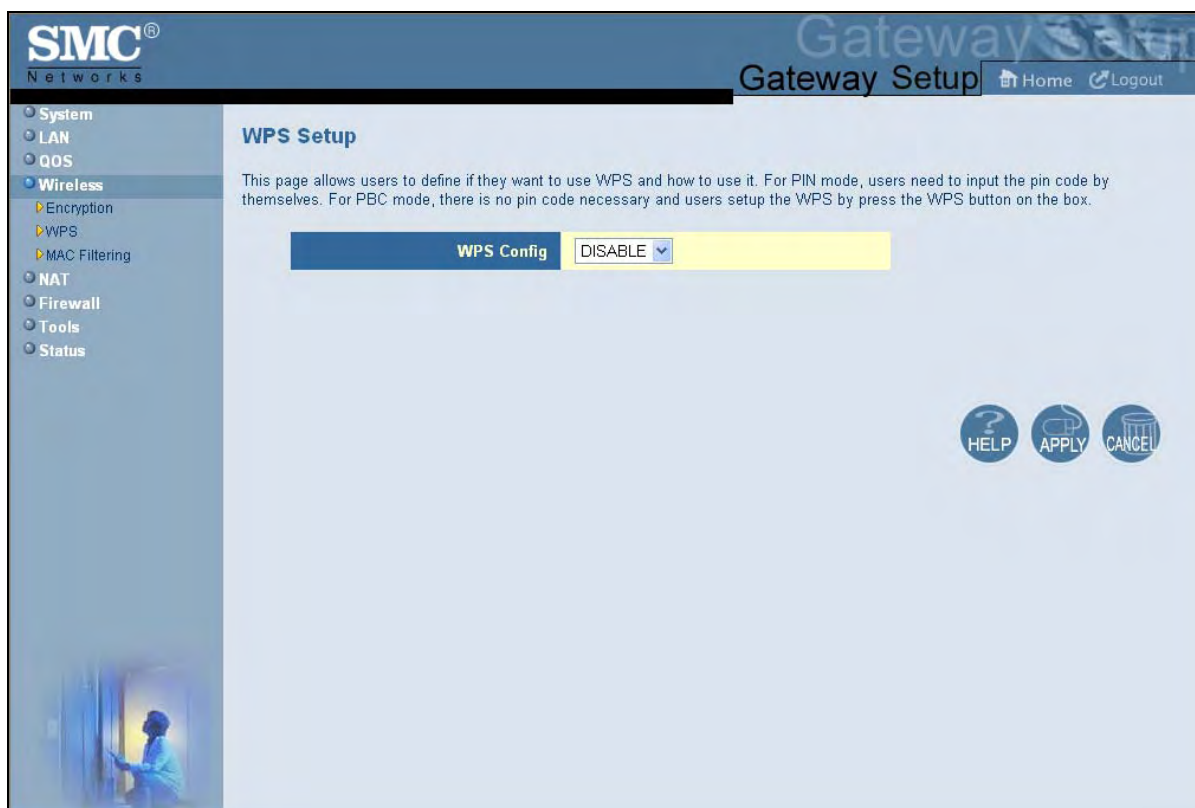


Figure 33. WPS Setup Menu

If you enable WPS configuration and click **Apply**, the menu options in Figure 34 appear. Table 13 describes the options shown.

Figure 34. WPS Setup Menu with WPS Config Enabled

Table 13. WPS Summary and WPS Progress Options

Option	Description
WPS Summary	
WPS Current Status	A read-only field that shows whether WPS is currently being used.
WPS Configured	A read-only field that whether WPS has been configured.
AP PIN	A read-only field that shows the personal identification number (PIN) for the access point.
WPS Progress	
WPS mode	<p>Determines whether WPS can be configured using a PIN or the WPS button on the front panel of the Gateway.</p> <ul style="list-style-type: none"> PIN = requires users to enter a PIN in the WPS Setup menu to configure WPS. PBC = Push Button Configuration. Allows users to use the WPS button on the front panel of the Gateway to configuring WPS.
WPS PIN	If PIN was selected for WPS mode, enter the PIN that users must enter to enable WPS. The PIN must be 8 alpha-numeric characters long.

MAC Filtering

Using the MAC Filtering menu, you can define up to 16 MAC address filters to prevent PCs from sending outgoing TCP/UDP traffic to the WAN via their MAC addresses. This is useful because a specific NIC's MAC address never changes, unlike its IP address, which can be assigned by a DHCP server or hard-coded to various addresses over time.

The MAC Filtering menu allows wireless client stations to connect over a wireless connection in two ways:

- By allowing all wireless station access.
- By allowing only trusted PCs.

To access the MAC Filtering menu, click **Wireless** in the menu bar and then click the **MAC Filtering** submenu. Figure 35 shows an example of the menu and Table 14 describes the settings you can select.



Note: The **MAC Filtering** submenu is not available in the menu bar if wireless operation is disabled in the Wireless Basic Settings menu (see page 40).

Figure 35. MAC Filtering Menu

Table 14. MAC Filtering Options

Option	Description
SSID	Network name of the of the primary wireless carrier.
MAC Filtering Mode	Determines which wireless client stations can connect to the Gateway. Te choices are: <ul style="list-style-type: none"> • Allow- All = all wireless client stations can connect to the Gateway. (<i>default</i>) • Allow = allow only the wireless client stations in the MAC filter table to connect to the Gateway. • Deny = no wireless client stations can connect to the Gateway.
Wireless Control List	Shows the device name and MAC address of up to 16 devices that you manually added to the MAC filter table. To delete a device, click the radio button to the left of the device you want to delete and click the Delete button. A precautionary message does not appear before deleting the MAC address, so be sure you do not need the MAC address before deleting it.
Auto-Learned Wireless Devices	Shows the wireless devices whose presence the Gateway has automatically learned.
Manually Added Wireless Devices	Enter a unique name and MAC address of the wireless devices that you want to manually add to the Wireless Control List (MAC filter table). Click Add to add the device to the Wireless Control List.

Adding and Deleting Wireless Client Stations

To allow wireless client stations to access the Internet through the Gateway, use the following procedure to define up to 16 wireless client stations.

- To add wireless client stations that the Gateway automatically learned on the network, perform the following steps under **Auto-Learned Lan Devices**:
 - Click a wireless client station that the Gateway learned automatically.
 - Click **Add**. The wireless client station is added to the **Wireless Control List**.
 - To add more auto-learned wireless client stations (up to 16), repeat steps 1a and 1b.
- To manually add wireless client stations, perform the following steps under **Manually-Added Wireless Devices**:
 - Under **Device Name**, enter a unique name for the device (that is, a name that does not already appear in the **Wireless Control List**).
 - Under **MAC Address**, enter the MAC address of the device.
 - Click **Add** to add the wireless client station to the **Wireless Control List**.
 - To manually add more wireless client stations (up to 16), repeat steps 2a through 2c.
- To delete wireless client stations from the **Wireless Control List** click the radio button corresponding to the wireless client station you want to delete and click the **Delete** button. A precautionary message does not appear before deleting a wireless client station.
- When you finish, click **Apply**.

Port Forwarding Menu

The Port Forwarding menu lets you configure your Gateway to provide port-forwarding services that let Internet users access predefined services such as HTTP (80), FTP (20/21), and AIM/ICQ (5190) as well as custom-defined services. You perform port forwarding by redirecting the WAN IP address and the service port to the local IP address and service port. You can configure a maximum of 100 predefined and custom-defined services.

To access the Port Forwarding menu, click **NAT** in the menu bar and then click the **Port Forwarding** submenu in the menu bar. Figure 36 shows an example of the menu.



Figure 36. Port Forwarding Menu

Adding a Port Forwarding Entry for a Predefined Service

Using the following procedure, you can select well-known services and specify the LAN host IP address(es) that will provide the service to the Internet.

1. In the Port Forwarding menu, click the **Add** button below the **Predefined Service Table**. The Predefined Service menu appears (see Figure 37).
2. Complete the fields in the Predefined Service menu (see Table 15).
3. Click **Apply**. (Or click **Back** to return to the Port Forwarding menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the predefined service is added to the **Predefined Service Table**.
4. To configure additional predefined services (up to 100, including customer-defined services), repeat steps 1 through 3.
5. To change the settings for a predefined service, click the radio button to the left of the service you want to change and click the **Edit** button. When the Predefined Service menu appears, edit the settings as necessary (see Table 15) and click **Apply**.
6. To delete a predefined service, click the radio button to the left of the service you want to delete and click the **Delete** button. No precautionary message appears before you delete a predefined service.

The screenshot shows the SMC Networks Gateway Setup web interface. On the left is a navigation menu with options: System, LAN, QOS, Wireless, NAT (selected), Port Forwarding, Firewall, Tools, and Status. The main content area is titled "Predefined Service" and includes a description: "Predefined service allows users to choose the traffic type to be allowed-in from Internet." Below this is a form with the following fields:

Service	AIM/ICQ(TCP:5190)
LAN Server IP	192.168.0.
Remote IPs	Any
Start IP	0.0.0.0
End IP	0.0.0.0

At the bottom of the form are three buttons: Back, Apply, and Cancel. A HELP icon is located in the bottom right corner of the main content area.

Figure 37. Predefined Service Menu

Table 15. Predefined Service Menu Options

Option	Description
Service	List of predefined services from which you can choose.
LAN Server IP	IP address of the LAN PC or server that is running the service.
Remote IPs	<p>Forwards the service to any remote IP address, one remote IP address, or a range of remote IP addresses.</p> <ul style="list-style-type: none"> • If you select one remote IP address, enter the IP address in the Start IP field. • If you select a range of remote IP addresses, enter the starting IP address in the Start IP field and the ending IP address in the End IP field.
Start IP	<p>To forward to:</p> <ul style="list-style-type: none"> • A single remote IP address, enter the remote IP address. • A range of remote IP addresses, enter the starting IP address here and the ending IP address range in the next field. <p>This field is unavailable if your Gateway is configured for any remote IP addresses.</p>
End IP	Enter the ending IP address in the remote IP address range. This field is unavailable if your Gateway is configured for any remote IP addresses or for a single remote IP address.

Adding a Port Forwarding Entry for a Customer-Defined Service

Using the following procedure, you can define special application services you want to provide to the Internet. The following example shows how to set port forwarding for a Web server on an Internet connection, where port 80 is blocked from the WAN side, but port 8000 is available.

Name:	Web Server
Type:	TCP
LAN Server IP:	192.168.0.100
Remote IPs:	Any (allow access to any public IP)
Public Port:	8000
Private Port:	80

With this configuration, all HTTP (Web) TCP traffic on port 8000 from any IP address on the WAN side is redirected through the firewall to the Internal Server with the IP address 192.168.0.100 on port 80.

To create your own customized services:

1. In the Port Forwarding menu, click the **Add** button below the **Customer Defined Service Table**. The Customer Defined Service menu appears (see Figure 38).
2. Complete the fields in the Customer Defined Service menu (see Table 16).
3. Click **Apply**. (Or click **Back** to return to the Port Forwarding menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the customer-defined service is added to the **Customer Defined Service Table**.
4. To configure additional customer-defined services (up to 100, including predefined services), repeat steps 1 through 3.
5. To change the settings for a customer-defined service, click the radio button to the left of the service you want to change and click the **Edit** button. When the Customer Defined Service menu appears, edit the settings as necessary (see Table 16) and click **Apply**.
6. To delete a customer-defined service, click the radio button to the left of the service you want to delete and click the **Delete** button. No precautionary message appears before you delete a customized service.

SMC[®] Networks Gateway Setup [Home](#) [Logout](#)

Customer Defined Service

Customer-defined service allows users to define their traffic type to be allowed-in from Internet.

Name	<input type="text"/>
Type	TCP
LAN Server IP	192 168 <input type="text"/> <input type="text"/>
Remote IPs	Any
Start IP	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
End IP	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Public IP Ports	Port Range
Start Public Port	<input type="text"/>
End Public Port	<input type="text"/>
Private Ports	<input type="text"/> <input type="checkbox"/> Enable Port Range

[Back](#) [Apply](#) [Cancel](#)

[? HELP](#)

Figure 38. Customer Defined Service Menu

Table 16. Customer Defined Service Menu Options

Option	Description
Name	Name for identifying the custom service. The name is for reference purposes only.
Type	The type of protocol. Choices are TCP, UDP, and TCP/UDP. Default is TCP.
LAN Server IP	IP address of the LAN PC or server that is running the service.
Remote IPs	<p>Forwards the service to any remote IP address, one remote IP address, or a range of remote IP addresses.</p> <ul style="list-style-type: none"> • If you select one remote IP address, enter the IP address in the Start IP field. • If you select a range of remote IP addresses, enter the starting IP address in the Start IP field and the ending IP address in the End IP field.
Start IP	<p>To specify:</p> <ul style="list-style-type: none"> • A single remote IP address, enter the remote IP address. • A range of remote IP addresses, enter the starting IP address here and the ending IP address range in the next field. <p>This field is unavailable if your Gateway is configured for any remote IP addresses.</p>
End IP	Ending IP address in the remote IP address range. This field is unavailable if your Gateway is configured for any remote IP addresses or a single remote IP address.
Public IP Ports	<p>A single public IP port or a range of public IP ports on which the service is provided. If necessary, contact the application vendor for this information.</p> <ul style="list-style-type: none"> • If you select a single public port, enter the port number in the Start Public Port field. • If you select a range of public ports, enter the starting port number in the Start Public Port field and the ending port number in the End Public Port field.
Start Public Port	Starting number of the port on which the service is provided.
End Public Port	Ending number of the port on which the service is provided. This field is unavailable if your Gateway is configured for a single public IP port.
Private Ports	Numbers of the ports whose traffic your Gateway forwards to the LAN. If there is a range of ports, enter the starting private port here and check Enable Port Range . The Gateway automatically calculates the end private port. The LAN PC server listens for traffic/data on this port (or these ports).

Security Settings (Firewall) Menu

The Security Settings (Firewall) menu lets you enable or disable your Gateway's firewall.

If you enable your Gateway firewall module, the following submenus appear in the menu bar:

- Configure access control settings — see page 69
- Configure your Gateway for special applications — see page 74
- Set up URL blocking — see page 77
- Schedule routes — see page 79
- Receive email or syslog alert notifications — see page 80
- Configure a local client computer as a local DMZ for unrestricted two-way Internet access — see page 84

Enabling or Disabling Firewall

The Security Settings (Firewall) menu provides an option for enabling or disabling your Gateway's firewall setting. To access the Security Settings (Firewall) menu, click **Firewall** in the menu bar. Figure 39 shows an example of the menu.

By default, your Gateway's firewall settings are enabled. To disable the firewall, uncheck **Enable Firewall Module** and click **Apply**. Disabling the firewall hides the submenus below the **Firewall** menu.

The Security Settings (Firewall) menu also provides an option for enabling or disabling the Session Initiation Protocol (SIP) application-layer gateway service on the Gateway firewall. This option allows SIP signaling requests to traverse directly through the Gateway to the destination device.

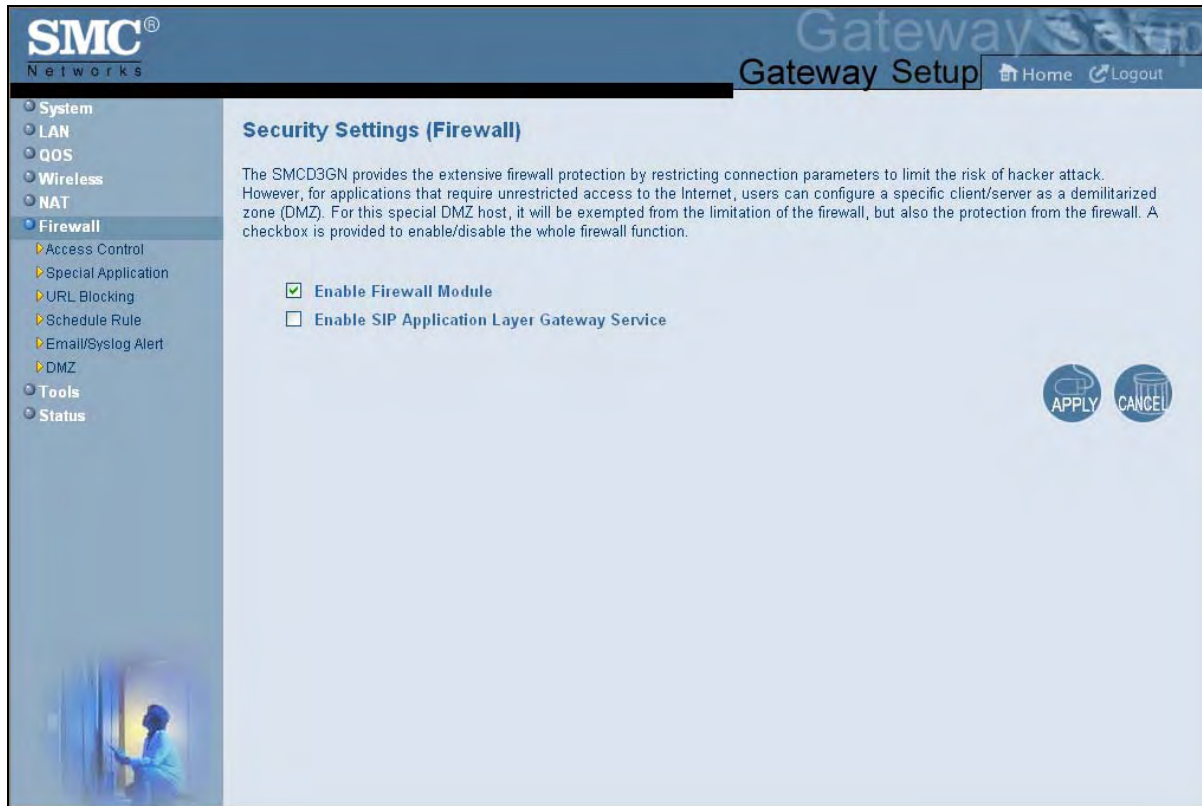


Figure 39. Security Settings (Firewall) Menu

Configuring Access Control

The Access Control menu lets you enable access control to block traffic at your Gateway's LAN interfaces from accessing the Internet.

To access the Access Control menu, click **Firewall** in the menu bar and then click the **Access Control** submenu in the menu bar.



Note: The **Access Control** submenu is not available in the menu bar if **Enable Firewall Module** is disabled in the Security Settings (Firewall) menu (see page 67).

To enable access control, check **Enable Access Control** if it is unchecked and click **Apply**. When Access Control is enabled, you can configure up to 35 predefined and customer-defined filtering tables.

SMC Networks Gateway Setup Home Logout

Access Control

By default all access attempts from the Internet to the LAN are blocked. In the NAT section, port forwarding rules can be setup to allow access from the Internet to the Private LAN. The following two Filtering Tables allow users to define the traffic type not permitted from LAN to the Internet. The maximum total number allowed for predefined and customer defined filters is 35

☒ **Enable Access Control**

The following two tables allow users to define the traffic type not-permitted from LAN site to the Internet. This page includes predefined IP filtering and customer-defined IP filtering. The maximum total number allowed for predefined and customer-defined filters is 35.

Predefined Filtering Table

#	Service Name	LAN IPs	Blocked
Add Edit Delete			

Customer Defined Filtering Table

#	Service Name	Type	LAN IPs	Port	Blocked
Add Edit Delete					

HELP APPLY CANCEL

Figure 40. Access Control Menu

Adding a Predefined Filter to Access Control

Using the following procedure, you can add predefined filters that block certain types of traffic from the LAN side of your Gateway to the Internet side of your Gateway.

1. In the Access Control menu, check **Enable Access Control** if it is not checked and click the **Apply** button. The remaining fields in the menu become available.
2. Under **Predefined Filtering Table**, click the **Add** button. The Predefined Filter menu appears (see Figure 41).
3. Complete the fields in the Predefined Filter menu (see Table 17).
4. Click **Apply**. (Or click **Back** to return to the Access Control menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the predefined filter is added to the **Predefined Filtering Table**.
5. To define additional filters for access control (up to 35, including customer-defined filters), repeat steps 1 through 4. When you finish, click **Apply** in the Access Control menu to save your settings.
6. To change the settings for a predefined filter, click the radio button to the left of the service you want to change and click the **Edit** button. When the Predefined Filter menu appears, edit the settings as necessary (see Table 17) and click **Apply**. Click **Apply** in the Access Control menu to save your settings.
7. To delete a predefined filter, click the radio button to the left of the filter you want to delete and click the **Delete** button. No precautionary message appears before you delete a predefined filter. Click **Apply** in the Access Control menu to save your settings.

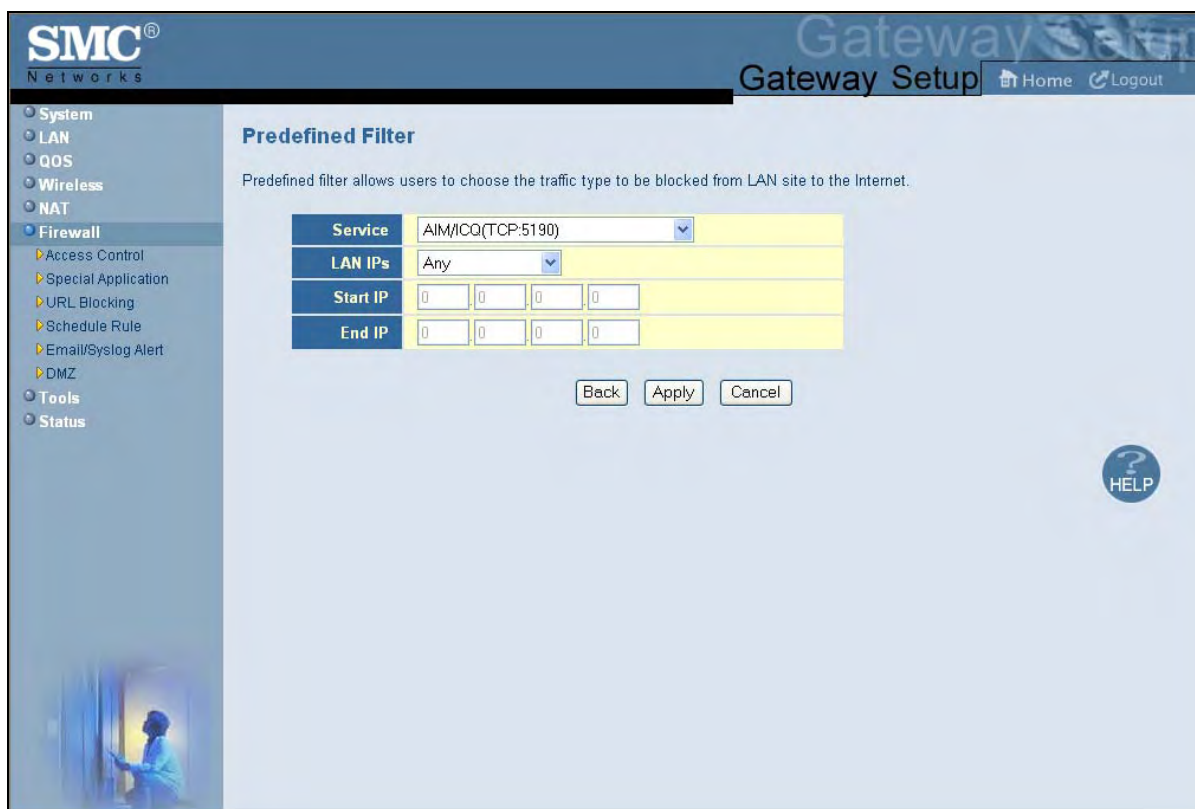


Figure 41. Predefined Filter Menu

Table 17. Predefined Filter Menu Options

Option	Description
Service	List of predefined services from which you can choose.
LAN IPs	<p>Lets you specify any LAN IP addresses, a single LAN IP address, or a range of LAN IP addresses to which the filter is applied.</p> <ul style="list-style-type: none"> If you select one LAN IP address, enter the IP address in the Start IP field. If you select a range of LAN IP addresses, enter the starting IP address in the Start IP field and the ending IP address in the End IP field.
Start IP	<p>To apply the predefined filter to:</p> <ul style="list-style-type: none"> A single LAN IP address, enter the LAN IP address. A range of LAN IP addresses, enter the starting IP address here and the ending IP address range in the next field. <p>This field is unavailable if your Gateway is configured for any LAN IP addresses.</p>
End IP	<p>Ending IP address in the LAN IP address range to which the filter will be applied. This field is unavailable if your Gateway is configured for any LAN IP address or a single LAN IP address.</p>

Adding a Customer-Defined Filter to Access Control

Using the following procedure, you can add customer-defined filters that block certain types of traffic from the LAN side of your Gateway to the Internet side of your Gateway.

1. In the Access Control menu, check **Enable Access Control** if it is not checked and click the **Apply** button. The remaining fields in the menu become available.
2. Under **Customer Defined Filtering Table**, click the **Add** button. The Customer Defined Filter menu appears (see Figure 42).
3. Complete the fields in the Customer Defined Filter menu (see Table 18).
4. Click **Apply**. (Or click **Back** to return to the Access Control menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the customer-defined filter is added to the **Customer Defined Filtering Table**.
5. To define additional filters for access control (up to 35, including predefined filters), repeat steps 1 through 4. When you finish, click **Apply** in the Access Control menu to save your settings.
6. To change the settings for a customer-defined filter, click the radio button to the left of the filter you want to change and click the **Edit** button. When the Customer Defined Filter menu appears, edit the settings as necessary (see Table 18) and click **Apply**. Click **Apply** in the Access Control menu to save your settings.
7. To delete a customer-defined filter, click the radio button to the left of the filter you want to delete and click the **Delete** button. No precautionary message appears before you delete a customer-defined filter. Click **Apply** in the Access Control menu to save your settings.

The screenshot shows the SMC Networks Gateway Setup web interface. The left sidebar contains a navigation menu with the following items: System, LAN, QOS, Wireless, NAT, Firewall (selected), Access Control, Special Application, URL Blocking, Schedule Rule, Email/Syslog Alert, DMZ, Tools, and Status. The main content area is titled "Customer Defined Filter" and includes a description: "Customer-defined filter allows users to define their traffic type to be blocked from LAN site to the Internet." Below this is a configuration table with the following fields:

Name	<input type="text"/>
Type	TCP
LAN IPs	Any
Start IP	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
End IP	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
From Port	<input type="text"/>
To Port	<input type="text"/>

At the bottom of the configuration area are three buttons: Back, Apply, and Cancel. A circular HELP button is located in the bottom right corner of the main content area.

Figure 42. Customer Defined Filter Menu

Table 18. Customer Defined Filter Menu Options

Option	Description
Name	Name for identifying the custom service. The name is for reference purposes only.
Type	The type of protocol you want to filter. Choices are TCP, UDP, and TCP/UDP. Default is TCP.
LAN IPs	<p>Lets you apply the filter to any LAN IP addresses, a single LAN IP address, or a range of LAN IP addresses.</p> <ul style="list-style-type: none"> • If you select one LAN IP address, enter the IP address in the Start IP field. • If you select a range of LAN IP addresses, enter the starting IP address in the Start IP field and the ending IP address in the End IP field.
Start IP	<p>To specify:</p> <ul style="list-style-type: none"> • A single remote IP address, enter the remote IP address. • A range of remote IP addresses, enter the starting IP address here and the ending IP address range in the next field. <p>This field is unavailable if your Gateway is configured for any remote IP addresses.</p>
End IP	Ending IP address in the LAN IP address range to which the filter will be applied. This field is unavailable if your Gateway is configured for any LAN IP address or a single LAN IP address.
From Port	Starting port number on which the filter will be applied. If necessary, contact the application vendor for this information.
To Port	Ending port number on which the filter will be applied. If necessary, contact the application vendor for this information.

Configuring Special Applications

Using the Special Application menu, you can configure your Gateway to detect port triggers for detect multiple-session applications and allow them to pass the firewall. For special applications, besides the initial communication session, there are multiple related sessions created during the protocol communications. Normally, a normal treats the triggered sessions as independent sessions and blocks them. However, your Gateway can co-relate the triggered sessions with the initial session and group them together in the NAT session table. As a result, you need only specify which protocol type and port number you want to track, as well as some other related parameters. In this way, your Gateway can pass the special applications according to the supplied information.

Assume, for example, that to use H.323 in a Net Meeting application, a local client starts a session A to a remote host. The remote host uses session A to communicate with the local host, but it also could initiate another session B back to the local host. Since there is only session A recorded in the NAT session table when the local host starts the communication, session B is treated as an illegal access from the outside and is blocked. Using the Special Application menu, you can configure your Gateway to co-relate sessions A and B and automatically open the port for the incoming session B.

To display the Special Applications menu, click **Firewall** in the menu bar and then click the **Special Application** submenu. Figure 43 shows an example of the menu.

The maximum allowed triggers is 50. To enable the special application function, check the **Enable Triggering** checkbox and click **Apply**. To disable it, uncheck the **Enable Triggering** checkbox and click **Apply**.



Note: The **Special Application** submenu is not available in the menu bar if **Enable Firewall Module** is disabled in the Security Settings (Firewall) menu (see page 67).



Figure 43. Special Applications Menu

To enable port triggering:

1. In the Special Application menu, check **Enable Triggering** if it is unchecked and click the **Apply** button. The Trigger Table becomes available.
2. Click the **Add** button below **Trigger Table**. The Trigger menu appears (see Figure 44).
3. Complete the fields in fields Trigger menu (see Table 19).
4. Click **Apply**. (Or click **Back** to return to the Trigger menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the trigger is added to the **Trigger Table**.
5. To configure additional triggers (up to 20), repeat steps 1 through 4. When you finish, click **Apply** in the Special Applications menu to save your settings.

6. To change the settings for a trigger, click the radio button to the left of the trigger you want to change and click the **Edit** button. When the Trigger menu appears, edit the settings as necessary (see Table 19) and click **Apply**. Click **Apply** in the Special Application menu to save your settings.
7. To delete a trigger, click the radio button to the left of the trigger you want to delete and click the **Delete** button. No precautionary message appears before you delete a trigger. Click **Apply** in the Special Application menu to save your settings.

The screenshot shows the SMC Networks Gateway Setup web interface. On the left is a navigation menu with categories: System, LAN, QOS, Wireless, NAT, Firewall (selected), Tools, and Status. Under Firewall, sub-items include Access Control, Special Application, URL Blocking, Schedule Rule, Email/Syslog Alert, and DMZ. The main content area is titled 'Trigger' and contains a form for configuring port triggers. The form fields are: Name (text input), Type (dropdown menu set to TCP), Trigger Port (From and To text inputs), Target Port (From and To text inputs), Interval (text input with a range of 50 ~ 30000 ms), IP Replacement (dropdown menu set to Disable address replacement), and Allow sessions initiated from/to the 3rd host (checkbox). Below the form are Back, Apply, and Cancel buttons. A HELP icon is in the bottom right corner.

Figure 44. Trigger Menu

Table 19. Trigger Menu Options

Option	Description
Name	Name for identifying the trigger. The name is for reference purposes only.
Type	The type of protocol you want to use with the trigger. Choices are TCP and UDP. Default is TCP. For example, to track the H.323 protocol, the protocol type should be TCP.
Trigger Port	From and To port ranges of the special application. For example, to track the H.323 protocol, the From and To ports should be 1720.
Target Port	From and To port ranges for the target port listening for the special application.
Interval	Specify the interval between 50 and 30000 between two continuous sessions. If the interval exceeds this time interval setting, the sessions are considered to be unrelated.

Option	Description
IP Replacement	Select the IP replacement according to the application. Some applications embed the source host's IP in the datagram and normal NAT would not translate the IP address in the datagram. To make sure the network address translation is complete, IP replacement is necessary for these special applications, such as H.323.
Allow sessions initiated from/to the 3 rd host	Decide whether the sessions can start from/to a third host. To prevent hacker attacks from a third host, this feature usually is not allowed. However, for some special applications, such as MGCP in a VOIP application, a session initiated from a third host is permitted. For example, assume Client A is trying to make a phone call to a host B. Client A tries to communicate with the Media Gateway Controller (MGC) first and provides host B's number to MGC. Then MGC checks its own database to find B and communicate with B to provide B the information about A. B uses this information to communicate directly to A. So initially, A is talking to MGC, but the final step has B initiating a session to A. If the third-party host-initiated session is not allowed in this example, the whole communication fails.

Configuring URL Blocking

Using the URL Blocking menu, you can configure your Gateway to block access to certain Web sites from local computers by entering either a full URL address or keywords of the Web site. your Gateway examines all the HTTP packets to block the access to those particular sites. This feature can be used to protect children from accessing inappropriate Web sites. You can block up to 50 sites.

Using URL blocking, you can also make up to 10 computers exempt from URL blocking and have full access to all Web sites at any time.

To display the URL Blocking menu, click **Firewall** in the menu bar and then click the **URL Blocking** submenu. Figure 45 shows an example of the menu.



Note: The **URL Blocking** submenu is not available in the menu bar if **Enable Firewall Module** is disabled in the Security Settings (Firewall) menu (see page 67).



Tip: The Gateway provides a Schedule Rules feature that lets you configure URL blocking for certain days, if desired. For more information, see “Configuring Schedule Rules” on page 79.



Figure 45. URL Blocking Menu

To enable URL blocking:

1. In the URL Blocking menu, check **Enable Keyword Blocking** if it is not checked and click **Apply**.
2. To exempt a computer from URL blocking, enter the computer's MAC address in the **Add exempted PC** field and click the **Add Trusted Host** button. The MAC address you entered appears in the **Exempted PC List**.
 - Repeat this step for each additional computer (up to 10) you want to make exempt from URL blocking.
 - To remove a computer from being exempted, use the **Delete** or **Delete All** buttons next to the field to delete selected or all MAC addresses.
3. To block a site, click in the **Keyword/Domain Name** field, enter keyword or domain name of the site you want to block, and click **Add Keyword**. The keyword or domain appears in the **Blocked Keyword/Domain List**.

- Repeat this step for each additional keyword or domain (up to 50) you want to make exempt from URL blocking.
- To remove a site from being blocked by a keyword or domain name, use the **Delete** or **Delete All** buttons next to the field to delete selected or all keywords and/or domains.

4. Click **Apply**.

Configuring Schedule Rules

Schedule rules work with your Gateway's URL blocking feature (described on page 77) to tell your Gateway when to perform URL blocking.

To access the Schedule Rule menu, click **Firewall** in the menu bar and then click the **Schedule Rule** submenu in the menu bar. Figure 46 shows an example of the menu.



Note: The **Schedule Rule** submenu is not available in the menu bar if **Enable Firewall Module** is disabled in the Security Settings (Firewall) menu (see page 67).

SMC Networks Gateway Setup

Home Logout

System

- LAN
- QOS
- Wireless
- NAT
- Firewall**
 - Access Control
 - Special Application
 - URL Blocking
 - Schedule Rule**
 - Email/Syslog Alert
 - DMZ
- Tools
- Status

Schedule Rule

This page defines the schedule rule you want to use with the "URL Blocking" page.

	Week Day
<input checked="" type="checkbox"/>	Every Day
<input checked="" type="checkbox"/>	Sunday
<input checked="" type="checkbox"/>	Monday
<input checked="" type="checkbox"/>	Tuesday
<input checked="" type="checkbox"/>	Wednesday
<input checked="" type="checkbox"/>	Thursday
<input checked="" type="checkbox"/>	Friday
<input checked="" type="checkbox"/>	Saturday

☒ All Day

Start Time: 12 (hour) 0 (min) AM

End Time: 12 (hour) 0 (min) AM

HELP APPLY CANCEL

Figure 46. Schedule Rule Menu

By default, your Gateway is configured to apply schedule rules to URL blocking 24 hours every day. To change these settings:

1. To change the days when schedule rules are applied to URL blocking, uncheck **Every Day** under **Week Day**. Then check the days when you want to apply schedule rules to URL blocking.
2. To change the hours when schedule rules are applied to URL blocking, uncheck **All Day**. Then specify the start and end times when you want to apply schedule rules to URL blocking. Select **AM** or **PM**, where AM refers to times from Midnight to Noon and PM refers to times from Noon to Midnight.
3. Click **Apply**.

Configuring Email and Syslog Alerts

The Gateway inspects packets at the application layer, and stores TCP and UDP session information, including timeouts and number of active sessions. This information is helpful when detecting and preventing Denial of Service (DoS) and other network attacks.

If you enabled your Gateway's firewall or content-filtering feature, you can use the Email/Syslog Alert menu to configure your Gateway to send email notifications or add entries to the syslog when:

- Traffic is blocked
- Attempts are made to intrude onto the network
- Local computers try to access block URLs

You can configure your Gateway to generate email notifications or syslog entries immediately or at a preconfigured time.

To access the Email/Syslog Alert menu, click **Firewall** in the menu bar and then click the **Email/Syslog Alert** submenu in the menu bar. Figure 47 shows an example of the menu. The menu has three sections:

- The top area lets you configure your Gateway to send email notifications.
- The middle area lets you configure the to add syslog entries.
- The bottom area lets you define the alerting schedule.



Note: The **Email/Syslog Alert** submenu is not available in the menu bar if **Enable Firewall Module** is disabled in the Security Settings (Firewall) menu (see page 67).

Gateway Setup

[Home](#)
[Logout](#)

- System
- LAN
- QoS
- Wireless
- NAT
- Firewall**
 - Access Control
 - Special Application
 - URL Blocking
 - Schedule Rule
 - Email/Syslog Alert**
 - DMZ
- Tools
- Status

Email/Syslog Alert

When the firewall feature is enabled, The user can be notified about the blocked traffic by email and/or syslog.

The SMCD3GN firewall can notify the user about the intrusion and/or the attempts to access the blocked URL, also the notification could be sent out immediately or by the predefined time schedule.

Mail Server Configuration

SMTP Server Address	<input type="text"/>
Sender's E-mail Address	<input type="text"/>

Mail Server Authentication

User Name	<input type="text"/>
Password	<input type="text"/>

Recipient list (up to 4 items)

	Name	Email Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>		

Syslog Server Configuration

Syslog Server Address	<input type="text"/>
-----------------------	----------------------

Alert Options

	Send Email	Send Syslog
When intrusion is detected	<input type="checkbox"/>	<input type="checkbox"/>

Figure 47. Email/Syslog Alert Menu

Configuring Email Alerts

The following procedure describes how to configure your Gateway to send email notifications. This procedure assumes that your mail server is working properly.

1. In the Email/Syslog Alert menu, under **Mail Server Configuration**, enter the following information:
 - **SMTP Server Address** = IP address of the SMTP server that will forward the email notification to recipients.
 - **Sender's E-mail Address** = name that will appear as the sender in the email notifications.
2. Under **Mail Server Authentication**, enter the following information:
 - **User Name** = your email name.
 - **Password** = your email password.
3. Under **Recipient list**, click **Add**. When the Recipient Adding menu appears (see Figure 48), enter the name of the person who will receive email notifications and the person's email address, and then click **Apply**. (Or click **Back** to return to the Email/Syslog Alert menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the email account is added to the **Recipient list**. To send email to additional email accounts (up to 4), repeat this step.
4. To change the settings for an email recipient, click the radio button to the left of the recipient you want to change and click the **Edit** button. When the Recipient Adding menu appears, edit the settings as necessary and click **Apply**.
5. To delete an email recipient, click the radio button to the left of the recipient and click **Delete**. No precautionary message appears before you delete the email recipient.
6. Click **Apply**.

Recipient Adding

Users could input and edit the email alert recipient list here.

Name	<input type="text"/>
Recipient's Email Address	<input type="text"/>

Figure 48. Recipient Adding Menu

Configuring Syslog Entries

To have your Gateway add a syslog entry when traffic is blocked, attempts are made to intrude onto the network, or local computers try to access block URLs:

1. In the Email/Syslog Alert menu, under **Syslog Server Configuration**, enter the syslog server address.
2. Click **Apply**.

Configuring Alert Options

Using the options in the **Alert Options** area, you can configure your Gateway to send an email to recipients you define in this menu and/or send entries to a syslog defined in this menu if your Gateway detects an intrusion.

To configure your Gateway to send an email to the configured email addresses if it detects an intrusion:

1. Perform steps 1 through 3 under “Configuring Email Alerts” on page 82.
2. Under **Alert Options**, check **Send Email**.
3. Click **Apply**.

To configure your Gateway to send an entry to a syslog if it detects an intrusion:

1. Perform step 1 under “Configuring Syslog Entries” on page 83.
2. Under **Alert Options**, check **Send Syslog**.
3. Click **Apply**.

Configuring DMZ Settings

If you have a local client computer that cannot run an Internet application properly behind the NAT firewall, you can configure it for unrestricted two-way Internet access by defining it as a Virtual Demilitarized Zone (DMZ) host. Adding a client to the DMZ may expose your local network to various security risks because the client in the DMZ is not protected by the firewall.

To access the DMZ (Demilitarized Zone) menu, click **Firewall** in the menu bar and then click the **DMZ** submenu in the menu bar. Figure 49 shows an example of the menu.



Note: The **DMZ** submenu is not available in the menu bar if **Enable Firewall Module** is disabled in the Security Settings (Firewall) menu (see page 67).

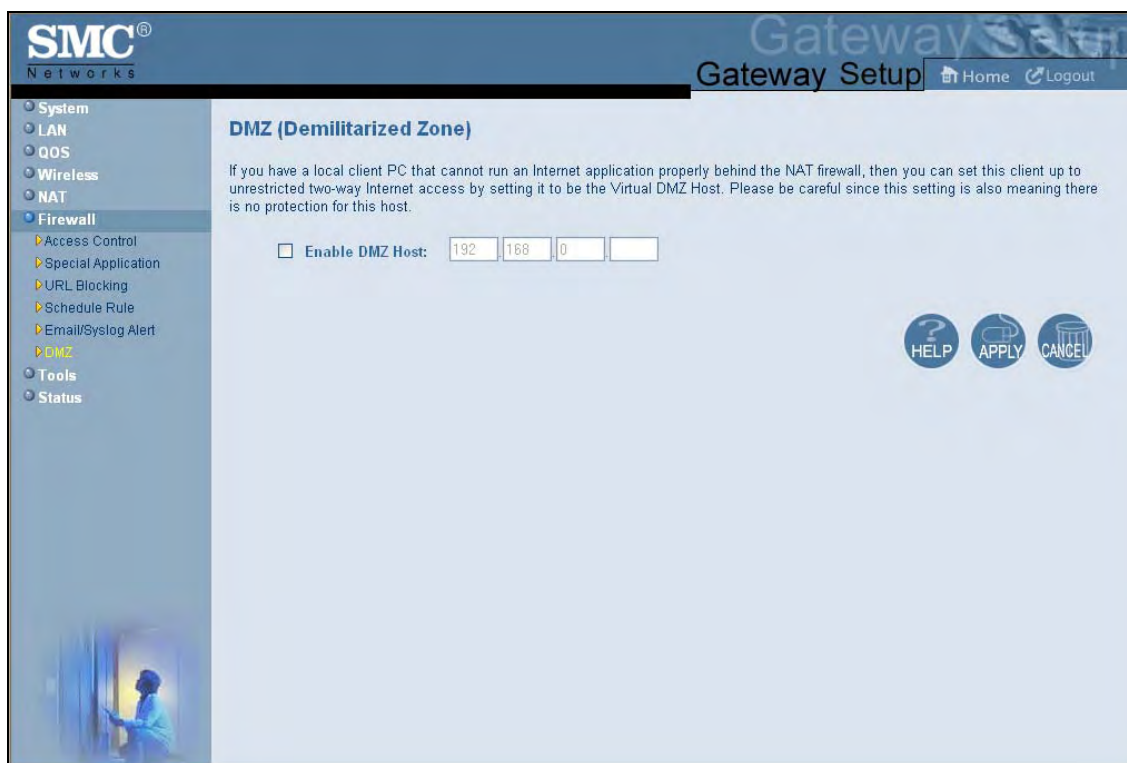


Figure 49. DMZ (Demilitarized Zone) Menu

To configure DMZ settings:

1. In the DMZ (Demilitarized Zone) menu, check **Enable DMZ Host**. The 2 rightmost fields next to this option become available.
2. Enter the last two octets in the IP addresses of the computer to be used as the DMZ server.
3. Click **Apply**.

Using the Reboot Menu to Reboot Your Gateway

Using the Reboot menu, you can reset your Gateway and retain all changes that have been made to your Gateway's factory default settings. To access the Reboot menu, click **Tools** in the menu bar and then click the **Reboot** submenu in the menu bar. Figure 50 shows an example of the menu.

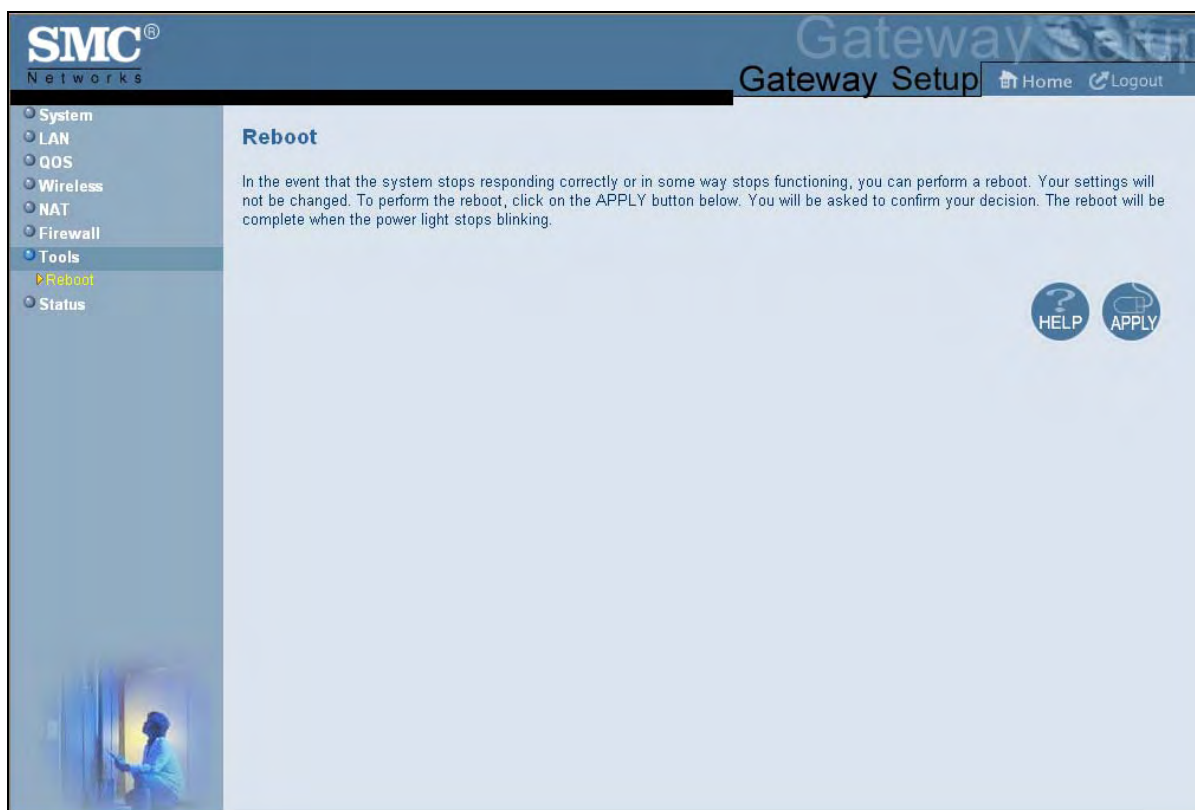


Figure 50. Reboot Menu

To reboot your Gateway and retain all changes made to its factory default settings:

1. In the Reboot menu, click **Apply**. The precautionary message in Figure 51 appears.
2. Click **OK** to reboot your Gateway or click **Cancel** to not reboot it. If you clicked **OK**, the reboot is complete when the **POWER** LED stops blinking and you will need to log in to the Web interface again.



Figure 51. Precautionary Message When Rebooting your Gateway

Using the Tools Settings Menu

Using the **Tools Settings** menu, you can reset the Gateway and restore the device's factory default settings. To access the Tools Settings menu, click **Tools** in the menu bar. Figure 52 shows an example of the menu.



Note: To reboot the Gateway and retain any customized settings, use the Reboot menu (see "Using the Reboot Menu to Reboot Your Gateway" on page 85).

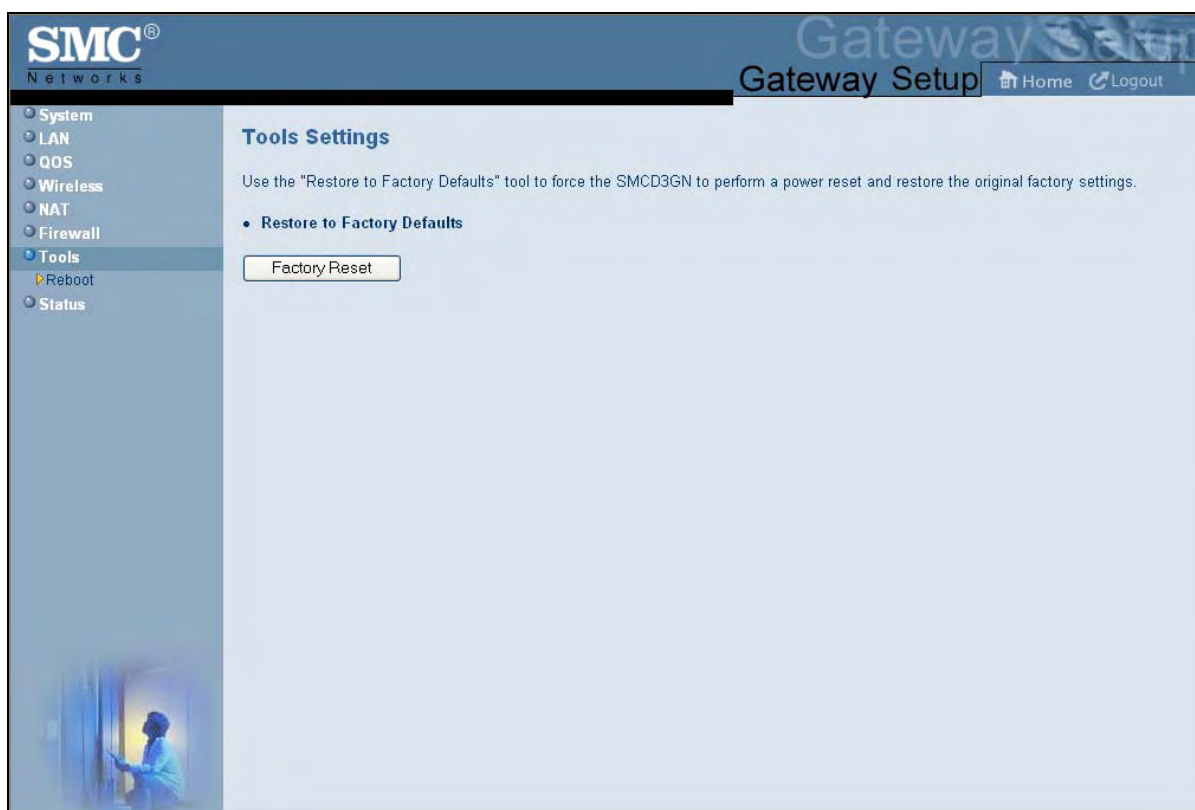


Figure 52. Tools Settings Menu

To reset the Gateway and restore its factory default settings:

1. Click **Factory Reset**. The warning message in Figure 53 appears.

2. Click **OK** to restore the Gateway's factory default settings or click **Cancel** to retain the Gateway's current settings.

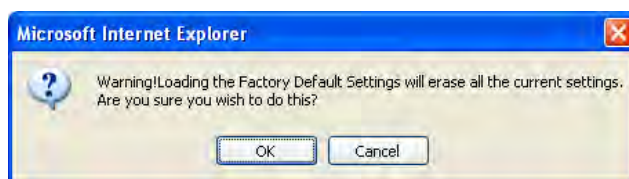


Figure 53. Warning Message when Restoring Factory Defaults

Using the Reboot Menu to Reboot the Gateway

Using the Reboot menu, you can reset the Gateway and retain all changes that have been made to the Gateway's factory default settings. To access the Reboot menu, click **Tools** in the menu bar and then click the **Reboot** submenu in the menu bar. Figure 50 shows an example of the menu.

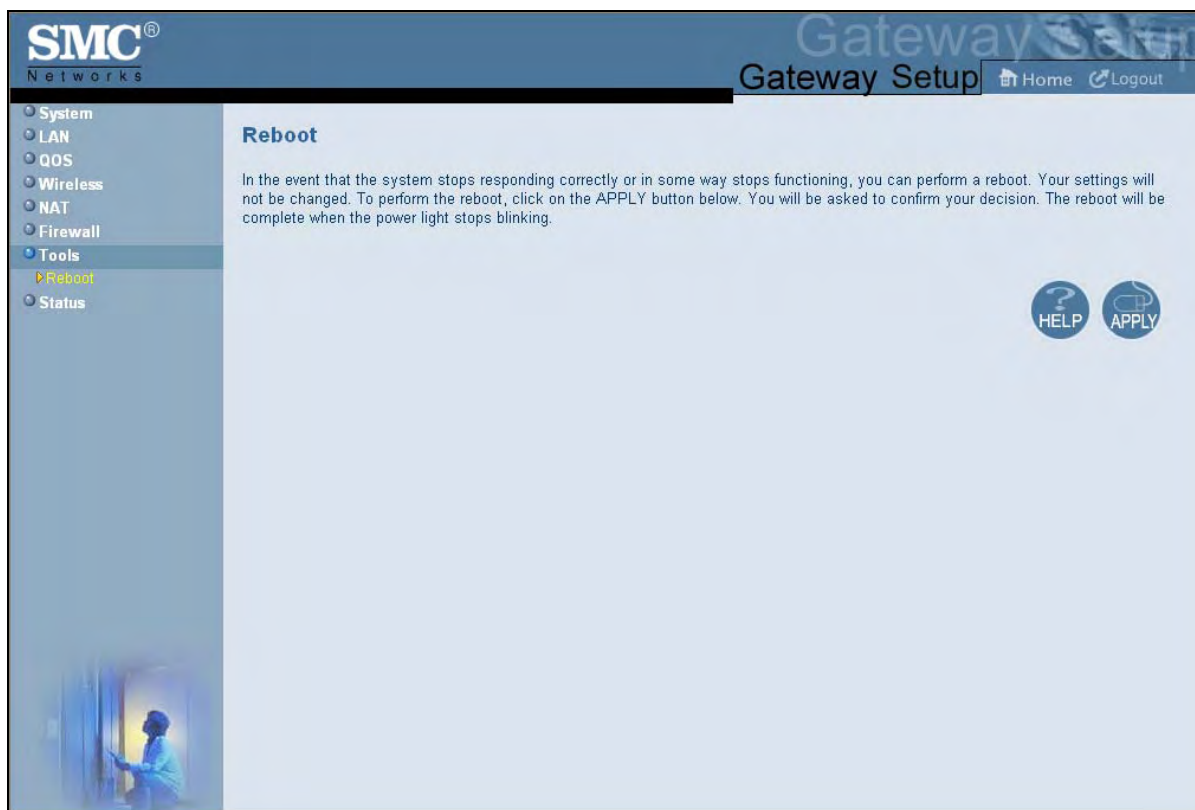


Figure 54. Reboot Menu

To reboot the Gateway and retain all changes made to its factory default settings:

1. In the Reboot menu, click **Apply**. The precautionary message in Figure 51 appears.

2. Click **OK** to reboot the Gateway or click **Cancel** to not reboot it. If you clicked **OK**, the reboot is complete when the **POWER** LED stops blinking and you will need to log in to the Web interface again.

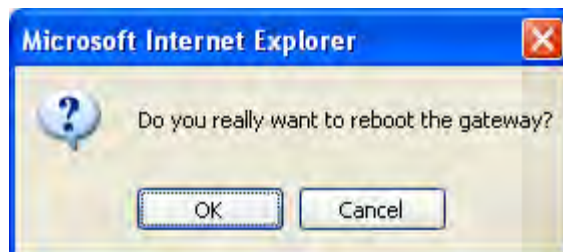


Figure 55. Precautionary Message When Rebooting the Gateway

Viewing Status Information

The Status page is a read-only screen that shows the:

- Connection status for your Gateway's WAN, LAN, and wireless interfaces
- Firmware and hardware versions
- Any illegal attempts to access your network
- Information about all DHCP clients currently connected to your Gateway
- Network and cable modem system event logs, with buttons for clearing, refreshing, or sending the logs to a drive location (before you can send the logs to a drive location, enable email and syslog notification on the Email/Syslog Alert menu - see page 80)
- LAN client log, with buttons for refreshing and releasing IP addresses

The Status menu appears when you first log in to the Web management interface. You can also display it by clicking **Status** in the menu bar. Figure 56 shows an example of the status information shown.

SMC® Networks Gateway Setup Home Logout

System
LAN
QoS
Wireless
NAT
Firewall
Tools
Status

Status

You can use the Status screen to see the connection status for the SMCD3GN WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your SMCD3GN.

RG Functions: Enabled
 NAT: Enabled
 DHCP Server: Enabled
 Firewall: Enabled

Current Time: Wed Jun 9 19:51:30 2010 System Up Time: 000 days 02h:03m:34s

INTERNET	GATEWAY	INFORMATION
WAN IP: 10.30.20.243	DHCP Gateway IP Address: 192.168.0.1	Model Name: SMCD3GN
WAN Subnet Mask: 255.255.255.0	Subnet Mask: 255.255.255.0	Software Version: 1.4.0.40-RRR
WAN Gateway IP: 10.30.20.1		Hardware Version: 1A
Primary DNS: 192.168.2.111	DNS Proxy IP Address: 192.168.0.1	RF Cable MAC Address: 00:22:2D:53:FA:75
Secondary DNS: 0.0.0.0		Wireless MAC Address: 00:22:2D:53:FA:79
		RG WAN MAC Address: 00:22:2D:53:FA:78
		Serial Num: H29260733C

WIRELESS
 SSID: D3GN_SSID0
 Encryption Type: No Encryption
 Encryption length: 0 Bits
 Encryption Pass Phrase: No Encryption
 Channel Being Used: 11

Interfaces Uptime and Traffic Count
 LAN Uptime: 02h:03m:33s ,Receiving 120 bytes ,
 Sending 361060bytes
 WAN Uptime: 02h:02m:23s ,Receiving 24312 bytes ,
 Sending 1170bytes

Network Log

View network activity and security logs.

```

(06/09/10 17:49:53) 10.224.1.10 comadmin Login Failed(Incorrect username
(06/09/10 17:50:26) 10.224.1.10 comadmin Login Failed(Incorrect username
(06/09/10 17:53:23) 10.224.1.10 rogcesadmin Login Failed(Incorrect usern
(06/09/10 17:53:25) 10.224.1.14 cusadmin Login Failed(deny)
(06/09/10 17:54:25) 10.224.1.14 cusadmin Login Success
(06/09/10 17:54:38) 10.224.1.14 cusadmin Logout
(06/09/10 19:51:09) 10.224.1.10 comadmin Login Failed(Incorrect username
(06/09/10 19:51:27) 10.224.1.10 cusadmin Login Success
  
```

Clear Refresh

LAN Client Log

View information on LAN clients currently linked to the SMCD3GN.

Refresh
 IP Release

Cable Modem System Event Log

View Cable Modem operation (start up, get time etc).

```

Time:01/01/70 00:00:57, Level:critical, Content:No Ranging Response rece
Time:06/09/10 17:48:59, Level:error, Content:Improper Configuration File
  
```

Clear Refresh

HELP

Figure 56. Example of Status Page

Viewing Cable Status Information

The Cable Status page is a read-only screen that shows the user's cable initialization procedures, along with the cable upstream and downstream status.

The Cable Status menu appears when you first log in to the Web management interface. You can also display it by clicking **Status** in the menu bar and then clicking the **Cable Status** submenu. Figure 57 shows an example of the cable status information shown.

SMC Networks Gateway Setup Home Logout

Cable Status

Cable status shows the users the cable initialization procedures, also the cable downstream and upstream status.

Initialization Procedure

Procedure	Status
Initialize Hardware	Success
Acquire Downstream Channel	Success
Upstream Ranging	Success
DHCP Bound	Success
Set Time-of-Day	Success
Downloading CM Config File	Success
Registration	Success

Traffic Enable!

Downstream Channel

ID	0	1	2	3
Downstream Frequency	621.001587 MHz	626.998413 MHz	632.999756 MHz	639.000977 MHz
Lock Status	Locked	Locked	Locked	Locked
Modulation	256 QAM	256 QAM	256 QAM	256 QAM
Symbol Rate	5.360537 Msym/sec	5.360537 Msym/sec	5.360537 Msym/sec	5.360537 Msym/sec
Downstream Power	-9.249801 dBmV	-9.168928 dBmV	-8.813492 dBmV	-9.468113 dBmV
SNR	37.935909 dB	37.092701 dB	37.935909 dB	38.257755 dB

Upstream Channel

ID	0	1	2	3
Upstream Frequency	30000000 Hz	10000000 Hz	20000000 Hz	38000000 Hz
Lock Status	Locked	Locked	Locked	Locked
Modulation	64QAM	64QAM	64QAM	64QAM
Symbol Rate	5120 sym/sec	5120 sym/sec	5120 sym/sec	5120 sym/sec
Upstream Power	50.0000 dBmV	51.0000 dBmV	51.0000 dBmV	51.0000 dBmV
Channel ID	15	13	14	16

HELP

Figure 57. Example of Cable Status Page

Appendix A - Specifications

Compatibility

- Platform independent – works with PC, OSX, Linux, MAC, UNIX
- DOCSIS 1.0/1.1/2.0/3.0 compliant
- IEEE 802.3, 802.3u
- SPI firewall meet ICSA guidelines

Network Interface

- 10/100/1000 Base-T-Ethernet
- USB2.0 port
- Wireless .11N MIMO

Ports

- Four ports 10/100/1000 MDI/MDIX auto sensing switch
- TR-68 coloring for 1 USB 2.0 Connector Type B
- TR-68 coloring for 4 Ethernet port
- Cable interface F type female 75 Ohm

Channel Bonding

- Downstream: up to 4 channels
- Upstream: up to 4 channels

Software Features

- GUI displays common troubleshooting information, modem status, and feature setup
- Full-featured CLI provides enhanced troubleshooting and setup
- DHCP server
- IPv6 support coexists with IPv4
- Downloadable configuration files allow for easy setup and installation.
- Universal Plug and Play (UPnP) enabling any UPnP devices seamlessly
- SAMBA for USB port connection of USB hard drives

- GUI/SNMP/CLI addition to present PHY usage (multiple channels parameters)
- Port Forwarding
- 64/256QAM auto detection
- Independent resets for downstream and upstream blocks
- Supports 64/128/256 bit RC4 authentication and encryption

Network Protocols

- IEEE 802.1d-compliant bridging
- DHCP Client/Server
- UDP
- DNS Relay
- ToD Client
- ARP
- ICMP
- FTP/TFTP
- Telnet

Security

- Password protected configuration access with multiple levels
- Stateful Packet Inspection (SPI) Firewall
- Network Address Translation (NAT)
- Application Level Gateways (ALG)
- Intrusion Detection
- Denial of Service (DoS) prevention
- Trojan Horse Prevention
- Smart Tracking
- VPN Passthrough (IPSec, PPTP, L2TP)
- Multiple User Profiles
- Dynamic Address-User Mapping
- Web-based authentication
- Comprehensive Logging
- Domain Validation
- Content and Filtering Features
- DMZ

Receiver

- Demodulation: 64/256QAM
- Input Frequency Range: 88MHz- 1002MHz
- Max speed: 38Mbps (64QAM) / 43Mbps (256QAM) per channel
 - DOCSIS 5120kbps/10Mbps (QPSK/16QAM)
 - DOCSIS 41.4 Mbps (64QAM)/55.2Mbps (256QAM)
 - Bounding (DOCSIS) per channel
- +222.48(+200) Mbps with 4 DS channel bounding (EuroDOCSIS)

Signal Level

- -15dBmV to +15dBmV (Automatic gain controlled by CM)
- 17 dBmV

Transmitter

- Modulation:
 - TDMA: QPSK, 8QAM, 16QAM, 32QAM, 64QAM, 128QAM
 - S-CDMA QPSK, 8QAM, 16QAM, 32QAM, 64QAM, 128QAM
- Max Speed 320, 640, 1280, 2560, 5120 kbps
- (QPSK), 640, 1280, 2560, 5120, 10240kbps (160QAM)
- +122.88(+108) Mbps with 4 US channel bounding (DOCSIS/EuroDOCSIS)

- Frequency Range: 5 to 42MHz (edge to edge) DOCSIS

LEDs

- Power
- DS (Downstream)
- US (Upstream)
- Online
- Link
- Diag
- WPS
- LAN (1-4)
- WiFi
- USB

Dimensions

- L x W x H: 26.8 x 15.5 x 3.5 mm (10.6 x 6.1 x 1.4 in)
- Weight: 930 g (2.05 lbs)

Input Power

- 12V/2A

Regulatory Certification

- FCC Part 15B Class B
- UL/cUL

Power Supply Energy Star Rating

- Level IV

Appendix B - Compliances

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IEEE 802.11b or 802.11g operation of this product in the U.S.A is firmware-limited to channels 1 through 11.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Note to CATV System Installer - This reminder is provided to call the CATV systems installer's attention to Section 820-93 of the National Electric Code which provide guideline for proper grounding and, in particular, specify that the Coaxial cable shield shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

Index

A

- Access control, 69
 - adding customer-defined filter, 72
 - adding predefined filter, 70
- Access Control menu, 69
- Adding
 - customer-defined filter for access control, 72
 - customer-defined service for port forwarding, 64
 - predefined filter for access control, 70
 - predefined service for port forwarding, 62
- Alert options, 83
- Alerts, 80
- Apple Macintosh TCP/IP configuration, 25
- Auto-negotiation, 40

B

- Blocking
 - domain, 79
 - keyword, 78

C

- Cable Status menu, 90
- Changing login password, 36
- Cipher type, 53
- Computer exempted from URL blocking, 78
- Configuration, 27
- Configuring
 - access control, 69
 - alert options, 83
 - auto-negotiation, 40
 - DHCP, 38
 - duplex mode, 40
 - email alerts, 82
 - firewall, 67

- idle timeout, 36
- login password, 36
- port forwarding, 61
- private LAN IP address, 38
- special applications, 74
- syslog entries, 83
- TCP/IP, 18
- wireless security, 13

Connecting

- LAN, 16
- WAN, 17

Conventions in this document, vii

CoS menu, 43

Customer-defined

- filter, 72
- service for port forwarding, 64
- service table, 61

D

DHCP setting, 38

Disabling

- firewall, 29
- LAN ports, 40
- security software, 29

Disabling proxy settings

- Firefox, 28
- Internet Explorer, 28
- Safari, 29

DMZ (Demilitarized Zone) menu, 84

Document

- conventions, vii
- organization, vii

Domain blocking, 79

DSCP Based QoS menu, 45

DSCP Remarking menu, 48

Duplex mode, 40

E

- Email alerts, 80, 82
- Email/Syslog Alert menu, 80
- Enabling LAN ports, 40
- Ether Switch Port Control menu, 40
- Exempted computers, 78

F

- Factory defaults
 - restoring, 14
- Firefox, disabling proxy settings, 28
- Firewall
 - configuring, 67
 - disabling, 29
- Front panel, 11
 - LEDs, 12

G

- Gateway
 - configuring, 27
 - connecting to the LAN, 16
 - connecting to the WAN, 17
 - front panel, 11
 - installing, 15
 - key features, vi
 - LEDs, 12
 - locating, 16
 - package contents, 10
 - powering on, 17
 - preconfiguring, 28
 - rear panel, 13
 - rebooting and losing custom settings, 14
 - specifications, 91
 - system requirements, 10
 - Web management, 30

I

- Idle timeout, 36
- Installation, 15
- Internet Explorer, disabling proxy settings, 28

K

- Key features, vi
- Keyword blocking, 78

L

- LAN connection, 16
- LAN ports, enabling or disabling, 40
- LAN Settings menu, 38
- Lease time, 38
- LEDs, 12
- Locating your Gateway, 16
- Logging in to Web management, 30
- Login password, 36

M

- MAC Filtering menu, 59
- Menus
 - Access Control, 69
 - Cable Status, 90
 - CoS, 43
 - DMZ (Demilitarized Zone), 84
 - DSCP Based QoS, 45
 - DSCP Remarking, 48
 - Email/Syslog Alerts, 80
 - Ether Switch Port Control, 40
 - LAN Settings, 38
 - MAC Filtering, 59
 - Password Settings, 36
 - Port Based QoS, 42
 - Port Forwarding, 61
 - QoS Settings, 41
 - Queue Settings, 46
 - Reboot, 85
 - Schedule Rules, 79
 - Security Settings (Firewall), 67
 - Special Application, 74
 - Status, 88
 - System Settings, 34
 - Tools Settings, 86
 - Trigger, 75
 - URL Blocking, 77

- Wireless Basic Settings, 51
- Wireless Encryption Settings, 53
- WPS Setup, 56

Menus in Web management, 32

Microsoft

- TCP/IP configuration for Windows 2000, 19
- TCP/IP configuration for Windows 7, 23
- TCP/IP configuration for Windows Vista, 21
- TCP/IP configuration for Windows XP, 20

P

Package contents, 10

Password Settings menu, 36

Password, changing, 36

Port Based QoS menu, 42

Port forwarding

- adding customer-defined service, 64
- adding predefined service, 62

Port Forwarding menu, 61

Port triggering, 75

Powering-on your Gateway, 17

Preconfiguration guidelines, 28

Predefined

- filter, 70
- service for adding port forwarding, 62
- service table, 61

Private LAN IP settings

- DHCP, 38
- domain name, 38
- IP address, 38
- IP subnet mask, 38
- lease time, 38

Proxy settings, 28

Q

QoS Settings menu, 41

Queue Settings menu, 46

R

RADIUS configuration, 36

Rear panel, 13

Rebooting

- losing custom settings, 14

Requirements, 10

Restoring factory defaults, 14

S

Safari, disabling proxy settings, 29

Schedule Rules menu, 79

Screens in Web management, 31

Security mode, 53

Security Settings (Firewall) menu, 67

Security software, 29

Security, configuring wireless, 13

Service table

- customer-defined, 61
- predefined, 61

Special Application menu, 74

Specifications, 91

SSID setting, 53

SSIDs, 51

Status menu, 88

Syslog

- alerts, 80
- entries, 83

System requirements, 10

System Settings menu, 34

T

TACACS configuration, 36

TACACS+ configuration, 36

TCP/IP configuration, 18

- Apple Macintosh, 25
- Microsoft Windows 2000, 19
- Microsoft Windows 7, 23
- Microsoft Windows Vista, 21
- Microsoft Windows XP, 20

Timeout for Web management session, 36

Tools Settings menu, 86

Trigger menu, 75

Triggering ports, 75

U

URL Blocking menu, 77

W

WAN connection, 17

Web management

 Access Control menu, 69

 Cable Status menu, 90

 CoS, 43

 DMZ (Demilitarized Zone) menu, 84

 DSCP Based QoS, 45

 DSCP Remarking, 48

 Ether Switch Port Control menu, 40

 LAN Settings menu, 38

 logging in, 30

 MAC Filtering menu, 59

 menus, 32

 Password Settings menu, 36

 Port Based QoS, 42

 Port Forwarding menu, 61

 QoS Settings menu, 41

 Queue Settings, 46

 Reboot menu, 85

 Schedule Rules menu, 79

 screens, 31

 Security Settings (Firewall) menu, 67

 Special Application menu, 74

 Status menu, 88

 System Settings menu, 34

 Tools Settings menu, 86

 Trigger menu, 75

 URL Blocking menu, 77

 URL Email/Syslog Alert menu, 80

 Wireless Basic Settings menu, 51

 Wireless Encryption Settings menu, 53

 WPS Setup menu, 56

Wireless

 mode, 51

 operation, 51

 security, 13

Wireless Basic Settings menu, 51

Wireless Encryption Settings menu, 53

WPA mode, 53

WPS Setup menu, 56



Technical Support

From USA and Canada (24 Hours a Day, 7 Days a Week)

Toll Free: 800-SMC-4YOU / 800-762-4968

Fax: 949-679-1481

Internet

Email Address: techsupport@smc.com

Driver Updates: http://www.smc.com/index.cfm?action=tech_support_drivers_downloads
www.smc.com

English: Technical Support information available at www.smc.com

English for Asia-Pacific: Technical Support information available at www.smc-asia.com

Deutsch: Technischer Support und weitere information unter www.smc.com

Espanol: En www.smc.com Ud. podra encontrar la informacion relativa a servicios de soporte tecnico

Francais: Informations Support Technique sur www.smc.com

Portugues: Informacoes sobre Suporte Tecnico em www.smc.com

Italiano: Le informazioni di supporto tecnico sono disponibili su www.smc.com

Svenska: Information om Teknisk Support finns tillgangligt pa www.smc.com

Nederlands: Technische ondersteuningsinformatie beschikbaar op www.smc.com

Polski: Informacje o wsparciu technicznym sa dostepne na www.smc.com

Cestina: Technicka podpora je dostupna na www.smc.com

Magyar: Muszaki tamogat informacio elerhető -on www.smc.com

简体中文: 技术支持讯息可通过www.smc-prc.com查询

繁體中文: 產品技術支援與服務請上 www.smcnetworks.com.tw

ไทย: สามารถหาข้อมูลทางด้านเทคนิคได้ที่ www.smc-asia.com

한국어: 기술지원관련 정보는 www.smc-asia.com을 참고하시기 바랍니다

Copyrights & Trademarks

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Document number: 14040RRR06092010